TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tutkintotyö

Ville Hirvimies

RFID-TEKNOLOGIA JA UHF-KÄSILUKIJAN SUUNNITTELU

Työn ohjaaja: Yliopettaja Jorma Punju
Työn valvoja: Toimitusjohtaja Pauli Tossavainen

Tampere 2008

Hirvimies, Ville RFID-teknologia ja UHF-käsilukijan suunnittelu
Tutkintotyö 52 sivua + 3 liitesivua
Työn ohjaaja Yliopettaja Jorma Punju
Työn valvoja Toimitusjohtaja Pauli Tossavainen
ToP Tunniste Oy
Kesäkuu 2008
Hakusanat RFID, UHF, lukija, SkyeTek

TIIVISTELMÄ

Tämän tutkintotyön aiheena on tutustua RFID-teknologiaan ja suunnitella radiotaajuisten etätunnisteiden (RFID) lukijalaitteen prototyyppi. Lukijassa käytetään SkyeTekin M9 UHF-moduulia. Työhön kuuluu myös laitteen sovittaminen USB 2.0 -liitäntään, kytkennän testaus ja moduulin tarjoamien I/O-liitäntöjen testaukseen tehtävä ohjelma.

Työn alussa tutustutaan RFID-teknologian historiaan. Tärkeimmät kehitysvaiheet käydään läpi 2. maailmansodasta aina nykypäivään asti. Teknologian kehitystä käydään läpi lähinnä käyttösovellusten myötä eri aikakausilla.

Seuraavaksi työssä käydään läpi RFID:n peruskäsitteet, joka antaa käsityksen teknologiassa käytettävistä komponenteista ja yleiskuvan niiden toiminnasta. RFID:n erilaisia sovelluskohteita esitellään myös tässä työssä ja tuodaan esille teknologian vahvuuksia ja heikkouksia. Työssä tutustutaan myös informaation turvaamiseen RFID-teknologiassa ja muutamiin tietoturvauhkiin.

Seuraava vaihe työssä on lukijan suunnittelu ja sen sovittaminen USB 2.0 -liitäntään. Lukijamoduulin I/O-liitäntöjen testaukseen tehdään ohjelma, jonka toiminta selvitetään. Prototyypin testaus käsitellään myös tässä kohdassa. Lopussa työstä tehdään yhteenveto ja pohditaan kehitystoimenpiteitä projektille

Hirvimies, Ville
Thesis
Thesis Instructor
Thesis Supervisor

RFID-technology and designing of UHF-handreader
52 pages, 3 appendices
Senior Lecturer Jorma Punju
Managing Director Pauli Tossavainen
ToP Tunniste Oy

May 2008
Keywords RFID, UHF, reader, SkyeTek

ABSTRACT

The subject of this thesis is get to know RFID technology and to design a prototype UHF-handreader. SkyeTek M9 UHF-module is used in the reader. Device adaptation to the USB 2.0 interface, device testing and the software to test the I/O-interfaces are also included in the thesis.

The first part of the thesis consists of RFID history. The most important highlights will be discussed from World War 2 to the present day. The technological progress is looked at mostly through different applications in different eras.

The second part consists of the basic concepts of the RFID technology which will give an outlook of the components used in the technology and general view of their usage. Different kinds of applications, pros and cons of the technology, information safekeeping and threats will be discussed in this part.

Designing the reader and its adaptation the USB 2.0 interface is discussed next. Software is made to test the I/O-interfaces of the module which functions will be explained. Testing the prototype is also discussed in this part. Synopsis is made at the end of the thesis and also some development ideas are brought up.

ALKUSANAT

Tämä tutkintotyö on tehty radiotaajuisen tunnistuksen alalla toimivalle ToP Tunniste Oy:lle. Haluan esittää kiitokseni ToP Tunniste Oy:n toimitusjohtajalle Pauli Tossavaiselle työn aiheen antamisesta ja työn eri osa-alueissa opastamisesta. Kiitän myös työn valvojana toiminutta yliopettaja Jorma Punjua.

Tampereella 19.5.2008

Ville Hirvimies

SISÄLLYSLUETTELO

LYHENTEET JA MERKIT

ABT	Adaptive Binary Tree, UHF-tunnisteiden törmäyksenestoprotokolla
ASK	Amplitude Shift Keying, amplitudimodulaatiomenetelmä
BAP	Battery Assisted Passive, puoliaktiivinen tunniste
BSE	Bovine Spongiform Encephalopathy, hullun lehmän tauti
EAS	Electronic Article Surveillance**,** 1960 -luvun lopussa kehitetty tuotteiden seurantajärjestelmä
EEPROM	Electronically Erasable Programmable Read-Only Memory, puolijohdemuisti, joka säilyttää datan ilman virtalähdettä ja tyhjentyy sähköisesti
EPC	Electronic Product Code**,** sähköinen tuotekoodi, joka on tallennettu RFID-tunnisteeseen
EU	Euroopan unioni, 27 eurooppalaisen jäsenvaltion muodostama taloudellinen ja poliittinen liitto
FDX	Full Duplex, samanaikainen tiedonsiirto molempiin suuntiin
FSK	Frequency Shift Keying**,** taajuusmodulaatiomenetelmä
HDX	Half Duplex, tiedonsiirto vuorottelee vastaanoton ja lähettämisen välillä
HF	High Frequency
HIB	Host Interface Board, SkyeTekin tekemä liitäntäkortti
IEC	International Electro-Technical Comission, kansainvälinen sähköalan standardointiorganisaatio
IFF	Identity Friend or Foe, Englannin sotilasoperaatio
ISM	Industrial, Scientific and Medical, vapaa taajuuskaista teollisuuden, tieteen ja lääketieteen käyttöön
ISO	International Organization for Standardization, kansainvälinen standardisoimisjärjestö

IT	Information Technology, informaatioteknologia
JTC 1	Joint Technical Committee number 1, tietotekniikan alalle perustettu työryhmä standardointiin
LF	Low Frequency
MAC	Media Access Control, Ethernet -verkon päätelaitteen fyysinen osoite
NRZ	Non-Return-to-Zero, binäärikoodaustapa
NVRAM	non-volatile RAM, muistipiiri, joka säilyttää datan sähkökatkoksenkin aikana
PCD	Proximity Coupling Device**,** lukijasta käytetty nimitys ISO 14443 -standardissa
PICC	Proximity Integrated Circuit Card, tunnisteesta käytetty nimitys ISO -14443 standardissa
PIE	Pulse Interval Encoding, koodaustyyppi ISO 18000-6 -standardissa
POS	Point of Sale
PPM	Pulse Position Modulation, ISO 15693 -standardissa käytetty modulaatiotapa
PSK	Phase Shift Keying**,** vaihemodulaatiomenetelmä
R/O	Read-Only
R/W	Read-Write
RFID	Radio Frequency Identification
SiRF	Yhtiö, joka valmistaa GPS-siruja ja ohjelmistoja
UHF	Ultra High Frequency
WORM	Write Once Read Many
WTO	World Trade Organization, maailman kauppajärjestö

1 Johdanto

Tämän työn tavoitteena oli perehtyä RFID-teknologiaan ja suunnitella UHF RFID -lukija. Työssä tutustutaan aihepiirin historiaan ja käydään läpi tämän tekniikan peruskäsitteitä, kuten standardeja, tunnisteet, lukijat, antennit ja käytössä olevat taajuusalueet. Työssä luodaan myös katsaus RFID-sovelluksiin ja tietoturvauhkiin.

Lukijassa käytetään SkyeTekin M9 UHF RFID -moduulia. Lukijan on tarkoitus olla helposti käytettävä ja saada tehonsa suoraan USB 2.0 -liitännästä. Moduulille tehdään myös oma testiohjelmistonsa, jolla ohjataan sen digitaalisia I/O-liitäntöjä.

SkyeTekin omaa SkyeWare 4.0 -ohjelmistoa, joka toimitetaan Development Kit -paketissa, käytetään työssä hyväksi testausvaiheessa. SkyeTekin omia kirjastoja ja kooditiedostoja käytetään testiohjelman teossa.

2 RFID:n historia

Vaikka teknologia on kehittynyt valtavasti ajan kuluessa ja RFID (*Radio Frequency Identification*) ei varmastikaan muistuta enää juurikaan sitä mitä se oli ennen, voidaan kuitenkin sanoa, että tekniikan ensiaskeleet otettiin jo ennen toista maailmansotaa.

Tutka, jonka keksi Sir Robert Alexander Watson-Watt, oli käytössä niin liittoutuneilla kuin saksalaisillakin. Tutkan käytössä suurin ongelma oli se, että ei ollut minkäänlaista tapaa tunnistaa vihollisen koneita omista koneista, jotka palasivat kotikentälle tehtävänsä suoritettuaan.

Saksalaiset keksivät ensimmäiseksi, miten tutkaa voitaisiin käyttää helposti koneiden tunnistukseen. Heidän ajatuksensa oli se, että jos konetta kääntäisi juuri tietyllä tavalla palatessaan tukikohtaan, se muuttaisi radiosignaalia, joka heijastui takaisin koneesta. Tämä melko alkeellinen tapa kertoi maassa olevalla tutka-asemalle, että palaavat koneet ovat saksalaisia. Voidaan siis sanoa, että heijastunut signaali oli ainutlaatuinen ja siksi myös tunnistettavissa omien koneesta saapuvaksi. Tähän periaatteeseen perustuvat myös nykyaikaiset passiiviset RFID-järjestelmät.

Myöhemmin Watson-Watt osallistui Englannin salaiseen projektiin, jonka tarkoituksena oli kehittää tunnistusjärjestelmä. Tuloksena oli maailman ensimmäinen aktiivinen RFID-järjestelmä IFF (*Identity Friend or Foe*). Järjestelmä toimi siten, että jokaiseen Englannin koneeseen asennettiin lähetin. Kun lähetin vastaanotti signaaleja tutka-asemalta maasta, alkoi se lähettää välittömästi omaa signaaliaan takaisin ja tunnistettiin omaksi koneeksi. RFID toimii nykyisin samalla tavalla. Signaali lähetään transponderille, joka lähettää oman signaalinsa takaisin lukijalle.

Kaupalliset sovellukset tulivat kuitenkin paljon sodan loppumisen jälkeen. Vasta 1960-luvulla yritykset alkoivat kehittää RFID-tekniikkaa myytäviksi sovelluksiksi. Knogo kehitti 1960-luvun lopulla niin sanotun ”yksi-bitti” tunnisteen, joka tunnetaan myös EAS (*Electronic Article Surveillance*) järjestelmänä. Järjestelmä toimi

yksinkertaisuudessaan siten, että asiakkaan ostaessa tuotteen kassalla kassahenkilö sammuttaa tagin. Toisin sanoen lukija muuttaa bitin nollaksi. Jos tuotetta ei osteta, bitti jää muuttamatta. Tällöin kaupan ovella olevat lukijat havaitsevat tagin ja soittavat hälytyksen. Tagit ovat vieläkin käytössä kuluttajapakkauksissa Searsilla ja JC Penneyllä Yhdysvalloissa. Tagit olivat suosittuja siksi, että ne tarjosivat erittäin tehokkaan varkaussuojan ja olivat edullisia. EAS -järjestelmä oli ensimmäinen laajalle levinnyt RFID-tekniikan käyttökohde.

Vuonna 1973 patentoitiin ensimmäinen kirjoitettava aktiivinen RFID-tunniste. Samana vuonna keksittiin myös sovellus, jolla voitiin avata ja sulkea ovi ilman avainta. Järjestelmä toimi siten, että avainkortin passiivinen transponderi lähetti oven läheisyydessä olevalle lukijalle signaalin. Kun lukija havaitsi oikean koodijonon avainkortilta, lukija avasi lukon. Samalla tavalla toimivat myös nykyisin käytössä olevat RFID-tunnisteilla toimivat lukot. Samalla vuosikymmenellä Yhdysvalloissa Los Alamosissa alettiin käyttää myös RFID-tekniikkaa ydinmateriaalin seurantaan. Kun kuljetusauto saapui tarkkaan vartioitujen tukikohtien portille, autossa oleva transponderi lähetti lukijalle oman identiteettinumeronsa ja mahdollisesti myös muuta tietoa, kuten autossa olevan lastin ja kuljettajan numeron. Oikeilla identiteettinumeroilla varustetut kuljetusautot saivat portit aukeamaan.

1980-luvulla saatiin markkinoille jo monia kaupallisia sovelluksia. Yhdysvalloissa nämä liittyivät lähinnä liikenteeseen, henkilöstöön ja eläimiin. Euroopassa keskityttiin lyhyen kantaman sovelluksiin liike-elämässä, eläinten tunnistuksessa ja teollisuudessa. Tietullit Italiassa, Ranskassa, Espanjassa, Portugalissa ja Norjassa alkoivat käyttää RFID-teknologiaa. Ensimmäinen näistä maista oli Norja, joka käynnisti toiminnan 1987. Pian Norjan jälkeen Yhdysvalloissa New Yorkin kaupungin busseja alettiin seurata RFID-tunnisteilla, kun ne ajoivat Lincolnin tunnelista.

Uusien sovellusten myötä alettiin tekniikan mahdollisuuksia ymmärtää paremmin ja keksiä uusia käyttökohteita. Los Alamosissa sijaitseva National Laboratory kehitti pian tietullisovellusten jälkeen Yhdysvaltojen maatalousministeriön pyynnöstä passiiviset RFID-tunnisteet, joita käytettiin seuraamaan lehmiä. Tarkoituksena oli

seurata, paljonko hormoneja ja lääkkeitä lehmille oli annettu kun ne olivat sairaina. Los Alamosissa kehitettiin passiivinen tunniste, joka toimi 125 kHz:n taajuusalueella. Tunniste vuorattiin lasisuojukseen, joka asetettiin lehmän nahan alle. Tunniste sai energiansa lukijasta ja heijasti oman, muunnellun signaalinsa takaisin tekniikalla, jota kutsutaan nimellä *Backscatter*. Tässä tekniikassa radioaalto heijastuu takaisin lähettäjälle. Ilmiötä voisi verrata vaikkapa peilistä heijastuvaan taskulampun valoon.

Myöhemmin kehitettiin HF (*High Frequency*) alueella toimivat tunnisteet. 13,56 MHz:n taajuusalueella toimivat tunnisteet tarjosivat suuremman kantaman ja tiedonsiirtonopeuden eivätkä ne olleet käytössä suurimassa osassa maailmaa. Tällä alueella toimii myös usein autojen varkaudenestojärjestelmä, jonka lukija on asetettu ohjauspyörään. Jos autoa yrittää käynnistää pelkällä avaimella ilman kuorta, jossa yleensä sijaitsee myös kaukosäätimellä toimivat lukitusjärjestelmä, auto ei käynnisty.

1990-luvulla IBM kehitti UHF (*Ultra High Frequency*) -taajuusalueella toimivan RFID-järjestelmän. Tämä antoi vieläkin paremman tiedonsiirtonopeuden ja kantaman. IBM aloitti pilottihankkeen Wal-Mart-ketjun kanssa mutta ei koskaan kaupallistanut tätä tekniikkaa, ja joutui myymään sen pois jouduttuaan taloudellisiin vaikeuksiin 1990-luvun puolivälissä.

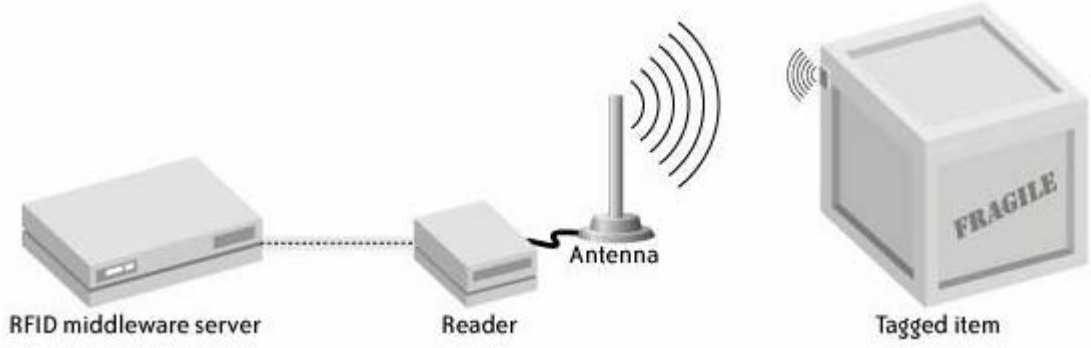
1999 perustettiin Auto-ID Center Massachusettsin teknilliseen korkeakouluun (MIT). Kaksi professoria, David Brock ja Sanjay Sarma, sai ajatuksen siitä, että asetettaisiin edulliset tunnisteet tuotteisiin. Näin niitä voitaisiin tarkkailla koko tuotteen toimitusketjun läpi. Ideana oli käyttää yksinkertaista mikrosirua, joka pystyi tallentamaan vain hyvin vähän informaatiota, vaikkapa yhden ainoan sarjanumeron tai ID-numeron. Tämä numero tallennettaisiin tietokantaan, joka olisi käytettävissä internetin välityksellä.

Nämä kaksi professoria muuttivat koko idean RFID-teknologiasta. Aikaisemmin ajatuksena oli ollut, että kaikki mahdollinen tieto, joka liittyisi tunnisteeseen, olisi fyysisesti luettavissa tunnisteesta. Nyt tunnisteesta ei tarvitsisi lukea kuin tietty ID-numero ja sen jälkeen kaikki informaatio voitaisiin hakea serveriltä internetin välityksellä. Tämä mahdollisti esimerkiksi sen, että tavarantoimittaja saattoi tarjota palvelua, jossa asiakas saattoi tarkastaa mihin kellonaikaan hänen tavaransa ovat lähteneet ja missä ne ovat pysähtyneet matkalla.

Auto-ID Center suljettiin vuonna 2003. Nykyään standardit RFID-teknologialle jakaa GS1 EPC Global. Suuret yritykset ja valtiohallinnon elimet ovat jo osoittaneet suurta mielenkiintoa RFID:lle. Näihin kuuluvat esimerkiksi Albertsons, Metro, Target, Tesco, Wal-Mart ja Yhdysvaltojen puolustusministeriö. Tulevaisuus RFID:n parissa näyttää lupaavalta ja uusia sovelluksia saatetaan markkinoille jatkuvasti. /2/

3 RFID teknologian peruskäsitteet

RFID kuvaa teknologiaa, jossa esineitä voidaan tunnistaa käyttämällä radioaaltoja tai magneettikenttiä hyödyksi. Esineisiin liitetään tunnisteet eli ”tagit”, jotka sisältävät informaation kyseisestä esineestä. Näitä tunnisteita voidaan lukea lukijoilla, jotka osaavat havaita kaikki tunnisteet sen omalla kantamalla. Lukija yleensä välittää tunnisteista saadun informaation toiselle järjestelmälle. Yleensä toisten sovellusten ja lukijan välissä on eräänlainen tulkkiohjelma, jota kutsutaan nimellä *RFID Middleware.* Kuva 1 esittää järjestelmän toiminnan yksinkertaisimmassa muodossaan.



Kuva 1. RFID-järjestelmä. /3/

3.1 Antennit

Antennin tehtävänä on lähettää ja vastaanottaa elektromagneettisia signaaleja tunnisteiden ja lukijan välillä. Elektromagneettista kenttää, jonka antenni lähettää, kutsutaan kuulustelualueeksi (*Interrogation Zone*). Antenni luo kolmiulotteisen tilan, jossa se kommunikoi tunnisteiden kanssa. Jotta kommunikaatiota tunnisteiden kanssa voisi tapahtua, täytyy tunnisteiden olla kuulustelualueella tai antennin kantoalueella. Antenneja saattaa olla useampia samassa kuulustelualueessa, mahdollistaen tunnisteiden lukemisen vaikeammissakin paikoissa. Antennit ovat usein suorakulmion muotoisia, ja niiden kotelot on suunniteltu suojaamaan niitä ulkopuolisilta vaikutteilta kuten pölyltä. Kuva 2 esittää tyypillisen RFID-antennin.

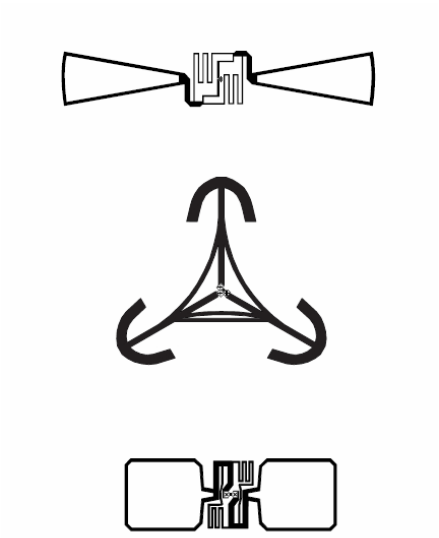
Kuva 2. Tyypillinen RFID-antenni. /6/

Antennien sijoittelu kohteessa ei ole aina aivan yksinkertaista. Esimerkiksi lastaussillalla antennit todennäköisesti sijoitettaisiin molemmille puolille kulkuaukkoa mutta trukissa antennin paikka olisikin kuljettajan yläpuolella runkoon asennettuna. Antennien sijainti korkeussuunnassa antaa myös mahdollisuuden säätää kuulustelualuetta. Yleensä sitä voidaan kasvattaa jonkin verran nostamalla antennia hieman maatasosta. Optimaalisen sijoituspaikan selville saamiseksi täytyy asennuskohteessa suorittaa testejä, onhan jokainen varastohalli, lastaussilta ja huone kuitenkin omanlaisensa.

Lukijan antenneista poiketen tunnisteiden antennit ovat täysin integroituja. Tagin antennia käytetään vastaanottamaan radiosignaaleja ja lähettämään niitä. Passiivisissa tunnisteissa antenni ottaa vastaan signaalin ja ohjaa sen tunnisteen piirille. Piirin vastaus saapuneeseen signaaliin lähetetään antennin kautta takaisin lukijalle. Antennin ulkomuotoon vaikuttaa se, mille taajuusalueelle tunniste on suunniteltu. HF-antennit ovat silmukkamaisia, kun taas UHF-antennit ovat tätä suorempia ja suurempia.

Toinen tärkeä asia tunnisteiden antenneissa muodon lisäksi on koko. Se vaikuttaa tunnisteen kykyyn absorboida RF-energiaa ja lähettää sitä. Koska yleensä tunnisteiden suunnittelussa ollaan kiinnostuneita kantamasta riippumatta sen tyypistä, tunnisteen fyysinen koko määrittyy suuresti antennin mukaan.

Tunnisteiden antennien tehokkuuteen vaikuttaa myös niiden sijoitustapa itse kohteeseen. Kaikki tuotteet eivät aina ole laatikoita, joten siksi hankaluuksia saattaakin ilmetä tunnisteen sijoittamisessa. Asiaa on yritetty korjata siten, että tunnisteisiin on lisätty useita antenneja tai haaroja. Kuvassa 3 on esitettynä muutamia antennimalleja. /1,2/



Kuva 3. Tunnisteiden antenneja. /7/

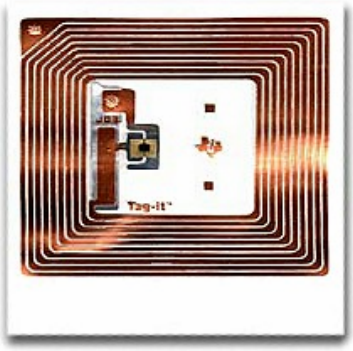
3.2 Tunnisteet

RFID tunnisteita valmistetaan erittäin monen muotoisina, kokoisina ja erittäin moneen käyttöön. Tästä syystä on mahdotonta kuvailla kaikkia mahdollisia tunnisteita mutta sen sijasta voidaan kuitenkin jakaa tunnisteet neljään kategoriaan niiden toiminnan perusteella: aktiivisiin-, puoliaktiivisiin-, passiivisiin- ja SAW-tunnisteisiin.

3.2.1 Passiiviset tunnisteet

Passiiviset tunnisteet ovat RFID:n kehityksen kärjessä nykypäivänä. Passiivisissa tunnisteissa ei ole lainkaan virtalähdettä. Ne saavat kaiken tarvitsemansa energian lukijan antennin tarjoamasta elektromagneettisesta säteilystä, jolla tunnisteessa oleva piiri toimii. Tästä syystä ne ovat myös yksinkertaisimpia rakenteiltaan ja huo-

mattavasti muita halvempia. Toinen hyvä puoli niissä on se, että ne ovat käytännössä ikuisia, koska ei ole mitään virtalähdettä, joka voisi kulua loppuun. Ne ovat myös pienempiä, joten käyttökohteita on huomattavasti enemmän kuin esimerkiksi aktiivisilla tunnisteilla. Kuvassa 4 on esitettynä tyypillinen passiivinen RFID-tunniste.



Kuva 4. Passiivinen HF RFID -tunniste. /8/

Passiivisia tunnisteita ei tarvitse huoltaa mitenkään käytössä, esimerkiksi niiden akkuja ei tarvitse vaihtaa. Tämä tarkoittaa sitä, että ne voidaan tarvittaessa valmistusvaiheessa sulkea hermeettisesti. Tämä tekee tunnisteesta erittäin kestävän. Näin ollen tunnisteita voidaan käyttää monissa sellaisissa kohteissa, joissa tavanomaisia tunnisteita ei voida, koska ne ovat huomattavasti herkempiä ympäristölle. Esimerkiksi hermeettisesti suljettu tunniste voitaisiin sijoittaa eläimen lapaluiden väliin ja sopivalla lukijalla voitaisiin tunnistaa eläimen omistaja. Toinen hyvä esimerkki on *Champion*-tunniste, joka sijoitetaan urheilijan jalkineisiin. Kotelonsa vuoksi tunniste kestää hyvin kosteutta ja siksi ei haittaa vaikka urheilusuorituksen aikana sataisikin vettä. Kun urheilija saapuu maaliin, siellä oleva RFID-antennimatto voi lukea tarkan maaliin saapumisajan. Tunniste on niin pieni, että se ei haittaa mitenkään itse urheilusuoritusta.

Haittapuolena passiivisissa tunneissa on ehdottomasti niiden erittäin rajallinen kantama. Nykytekniikalla tunnisteiden on oltava melko lähellä lukijaa, jotta ne saavat tarpeeksi energiaa omaan piiriinsä lähettääkseen signaalin takaisin. Kantaman pienuus voi myös olla hyvä asia tietoturvan kannalta. Monikaan kauppias ei varmasti-

kaan haluaisi, että koko varaston inventaarin voisi joku ulkopuolinen saada tietoon monien kymmenien metrien päästä. Usein kantaman pienuus ei haittaa. Lukija voidaan helposti sijoittaa lähemmäksi tunnistetta. On myös sellaisia tapahtumia, jossa kantaman riittämättömyys voi koitua huomattavaksi ongelmaksi. Urheilutapahtumissa onkin annettu suositukseksi, että käytössä olisi aina 2 antennimattoa, jotta saataisiin maksimoitua lukuvarmuus mahdollisimman lähelle 100 %:a.

Passiivisten tunnisteiden toisena haittana voidaan pitää pientä informaation säilytyskykyä. Monestikin tunnisteet kykenevät vain toistamaan maksimissaan kymmenestä merkistä koostuvan jonon. Näissä tapauksissa on oltava jokin ulkoinen tietokanta, johon tunnisteen lähettämää informaatiota voitaisiin verrata. Vain siten tiedosta tulee merkityksellinen, koska jono *xytag7389l* itsessään ei kerro kovinkaan paljon. E-passi edustaa varmaankin kehittyneintä tekniikkaa passiivisissa tunnisteissa nykypäivänä. Tunniste, joka on laitettu passin kuoriin, sisältää henkilön nimen, syntymäpäivän, syntymäpaikan, passin numeron ja jopa valokuvan hänestä. Kaikki data passilla on salattua (kryptattua), ja se voidaan lukea vain tietyllä avaimella. Kuitenkin tämäkin tietomäärä on vähäistä verrattuna aktiivisiin tunnisteisiin.

RFID-teknologian suurimpia haasteita menneinä vuosina on ollut juuri tunnisteiden liian korkeat hinnat. Siksi kehitystyö passiivisten tunnisteiden parissa on juuri nyt lupaavaa, kun valmistushinnat laskevat ja lukuetäisyydet kasvavat. /1,2/

3.2.2 Aktiiviset tunnisteet

Aktiivisissa tunnisteissa on aina virtalähde mukana. Yleensä se on jonkinlainen paristo. Tämä paristo tai akku antaa tarvittavan tehon sekä antennille että piirille. Pariston takia myös tunnisteen fyysinen koko on suurempi kuin passiivisen tunnisteen. Aktiivisissa tunnisteissa onkin usein muoviset kuoret, minkä vuoksi niitä ei voida liimata tai muutenkaan kiinnittää yhtä helposti tuotteisiin kuin filmi- tai Mylar-pohjaista passiivista tunnistetta. Kuvassa 5 on esitettynä seurantaan tarkoitettu aktiivinen RFID-tunniste.

Kuva 5. Aktiivinen RFID-tunniste. /9/

Virtalähteen ansiosta aktiivisten tunnisteiden kantama on paljon suurempi kuin passiivisten tunnisteiden. Se voi olla jopa satoja metrejä, passiivisilla tunnisteilla sen jäädessä usein kymmeniin sentteihin ja maksimissaankin vain muutamiin metreihin.

Aktiivisten tunnisteiden virtalähdettä säästetään siten, että tunniste sammuu silloin kun se ei ole kuulustelualueella. Kun tunniste saapuu alueelle, se aktivoituu automaattisesti ja tarjoaa siten informaation järjestelmälle. Koska tunniste on sammutettuna silloin kun ei olla kuulustelualueen sisäpuolella, virtalähteen toiminta-aikaa voidaan suuresti kasvattaa. Tosin aktiivinen RFID-järjestelmä on suunniteltava siten, että tunnistetta ei lueta kuin kerran alueelle saavuttuaan ja sen jälkeen se sammutetaan välittömästi. Muutoin virtalähde jäisi toimimaan ja laite lähettäisi signaaliaan niin kauan kuin virtalähde tyhjentyisi.

Ominaisuuksiensa vuoksi aktiiviset tunnisteet voivat olla myös hieman kehittyneempiä kuin passiiviset tunnisteet. Joissain tapauksissa tunnisteissa voi olla mukana myös jotain aivan muuta tekniikkaa, kuten esimerkiksi GPS-vastaanotin integroituna. Nykyään vastaanotin voi olla matkapuhelimissa (SiRF), radioissa ja jopa kelloissa, joten sen integroimisesta tuotteisiin on jo paljon kokemusta. Tällä tekniikalla voidaan esimerkiksi merikontti paikallistaa muutamien metrien tarkkuudella maailmassa ja saada tunnistetiedot kontista.

Aktiivisten tunnisteiden suuren koon ja kalliimman hinnan vuoksi niitä ei voida käyttää kooltaan pienissä tuotteissa, eikä varsinkaan massatuotteissa. Tästä syystä niitä tuskin koskaan käytetään kulutustuotteissa. /2,3/

3.2.3 Puoliaktiiviset tunnisteet

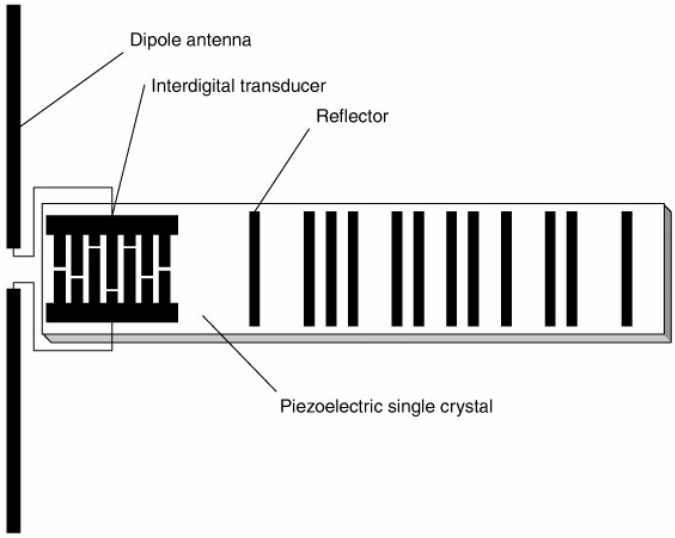
Puoliaktiiviset tunnisteet on suunniteltu siten, että niistä löytyy sekä passiivisten että aktiivisten tunnisteiden ominaisuuksia. Usein näitä nimitetään myös puolipassiivisiksi- tai BAP- (*Battery Assisted Passive*) tunnisteiksi. Tällä tavoin yritetään saada molempien tekniikoiden hyvät puolet käyttöön eliminoimalla samalla huonot puolet tekemällä eräänlainen hybriditunniste.

Tunnisteisiin voidaan myös asettaa erilaisia antureita tarkkailemaan esimerkiksi kosteutta tai liikettä. Tunniste voi siten tallentaa lämpötilanvaihtelut elintarvikekuljetuksen aikana, ja ne voidaan lukea terminaalissa. Toisaalta tunniste voi tallentaa paketin liikkeet kuljetuksen aikana, mikä mahdollistaa sen, että rikkoutuneet tuotteet saadaan helposti karsittua pois kuormasta.

Puoliaktiiviset tunnisteet eivät yleensä käytä virtalähdettään ollenkaan kommunikointiin antennin kanssa kuten aktiiviset tunnisteet. Tältä osin se siis toimii täysin samalla tavalla kuin passiivinen tunniste, ja tarvittava energia kommunikointiin lukijan kanssa saadaan elektromagneettisesta kentästä. Näin saadaan suuresti säästettyä sisäistä virtalähdettä kasvattaen sen käyttöikää. Tosin sovelluksissa, joissa tarvitaan ajoittain lisätehoa signaalin lähetykseen, käytetään myös puoliaktiivisia tunnisteita. Esimerkiksi lavallisesta laatikoita saadaan uloimmat luettua jokseenkin helposti mutta keskimmäiset laatikot saattavat aiheuttaa ongelmia. Ongelma ei ole siinä, että lukijan teho ei riittäisi yltämään tunnisteisiin vaan siinä, että passiivisen tunnisteen teho ei riitä vastaukseen. Siksi joskus tarvitaan myös ylimääräistä tehoa antennin kanssa kommunikointiin. /2,3/

3.2.4 SAW-tunnisteet

SAW (*Surface Acoustic Wave*) -tunnisteet ovat passiivisia, mutta ne kuitenkin toimivat aivan omalla tavallaan. Tyypillisesti RFID-tunnisteet perustuvat puolijohdefysiikkaan tuottaakseen tarvittavan tehon kommunikointiin lukijan kanssa. SAW-tunnisteet muuttavat tulevan radioaallon nanoluokan kokoisiksi pinta-akustisiksi aalloiksi piirin pinnalle. Kuvassa 6 on esitettynä tunnisteen osat.

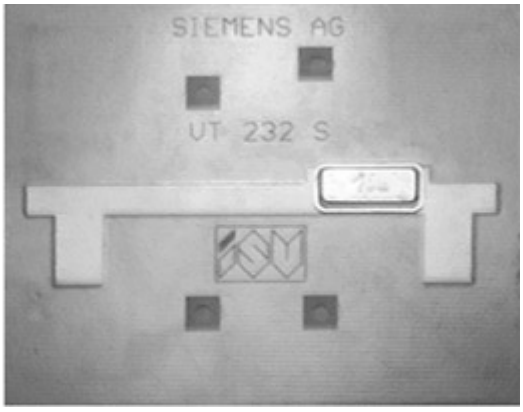


Kuva 6. SAW-tunnisteen osat. /1/

Aalto liikkuu pituussuunnassa pitkin tunnistetta. Osa aallosta heijastuu takaisin jokaisesta reflektorista. Loput aallosta absorboituu tunnisteen päätyyn. Heijastuneet aallot matkaavat takaisin muuntajalle (*Interdigital transducer*), jossa ne muutetaan korkeataajuisiksi pulssijonoiksi ja lähetetään sen jälkeen antennilla takaisin lukijalle. Pulssien määrä perustuu tunnisteen reflektorien määrään. Pulssien välinen viive on myös suoraan verrannollinen reflektorien väliseen matkaan, joten välimatkaa muuttelemalla voidaan vaikuttaa tunnisteen lähettämään binäärilukusarjaan.

Pinta-aaltojen hitaan kulkuajan vuoksi ensimmäinen pulssi vastaanotetaan lukijalla noin 1,5 ms:n kuluttua siitä, kun skannauspulssi on lähetetty. Tämä on erittäin hyvä asia, koska skannauspulssi heijastuu takaisin lukijaan myös ympäristöstä ja etenkin

metalliesineistä. 100 metrin päässä olevasta metalliesineestä heijastunut aalto matkaa valonnopeudella takaisin lukijaan vaimentuneena yli 160 dB. Edestakaiseen matkaan kuluu aikaa noin 0,6 ms, joten kun odotettu pulssi tunnisteesta tulee takaisin lukijalle, ovat kaikki ympäristöstä heijastuneet lähetteet poistuneet. Näin vältytään lukuvirheiltä, joita muutoin varmasti tulisi. Kuvassa 7 on esitettynä Siemensin SAW-tunniste. Pietsokide on asetettu metallikoteloon, jossa se on suojattu ympäristöltä.



Kuva 7. Siemensin SAW-tunniste. /1/

Datan varastoimiskyky tunnisteella on riippuvainen sen fyysisestä koosta ja etäisyydestä lukijaan. Yleensä 16 - 32 bittiä saadaan siirrettyä 500 kbit/s nopeudella. Toimintataajuus SAW-tunnisteilla on mikroaaltoalueella eli 2,45 GHz.

SAW-tunnisteiden lukuetäisyyteen vaikuttaa olennaisesti lukijan teho. ISM-hyväksytyillä tehotasoilla päästään 2,45 GHz:n alueella yleensä 1 - 2 metrin lukuetäisyyksiin. Lukuetäisyys ja tunnisteen lämpötila voidaan myös mitata samalla kun tunnistetta luetaan. SAW-tunnisteet voivat toimia moitteettomasti -100 °C:sta aina +200 °C:een asti. Ne kestävät myös röntgen- ja gammasäteilyä. /1,2/

3.3 Standardit

Standardit määrittelevät useita asioita, jotka tekevät RFID-teknologiasta käyttökelpoisen ympäri maailmaa. Informaation rakenteen standardoinnilla voidaan määritellä kuinka dataa käsitellään ja tallennetaan. Ilmarajapinnan protokollat määrittelevät tavan, jolla tunnisteet kommunikoivat. Testauksen standardoiminen takaa, että kaikki tuotteet täyttävät hyväksyttävät normit. Käyttösovelluksien standardoimisella määritellään miten erilaisia laitteita kuten lukijoita käytetään.

ISO (*International Organization for Standardization*) on kansainvälinen järjestö, jonka jäsenenä on 148 valtiota. Jokaisesta valtiosta on yksi edustaja. ISO perustettiin vuonna 1947, ja sen päämaja on Sveitsissä Geneven kaupungissa. Päätösten keskittäminen yhteen järjestöön antaa mahdollisuuden siihen, että standardit olisivat kansainvälisesti yhteensopivia, yhteneviä ja selkeitä. ISO jakaa standardeja moniin sovelluksiin ja myös RFID-tekniikkaan.

Päätökset RFID-tekniikkaa koskevista ISO-standardeista tekevät kaksi ryhmittymää. ISO ja IEC (*International Electro-Technical Comission*) muodostavat yhdessä JTC 1:n (*Joint Technical Committee number 1*), jolla on monia alakomiteoita.

3.3.1 ISO/IEC 18000 -standardijoukko

Vaikka monia standardeja on RFID-tekniikasta jo olemassa, niistä ehkäpä tärkeimmäksi ilmarajapintaa käsiteltäessä on juuri ISO/IEC 18000 -standardijoukko, joka koskee juuri esineiden tunnistusta.

ISO 18000-1 -standardi määrittelee pohjan kaikille 18000-sarjan standardeille. Muut osat tästä standardista määrittelevät tarkemmin esimerkiksi eri taajuusalueet ja niiden erityispiirteet. Tämä standardi on rajoitettu koskemaan datan siirtoa ilmarajapinnassa. Mitään tapoja, laitteita tai ohjelmistoja ei määritellä tässä standardissa, vaan yksinkertaisesti se, miten datan siirto tulee tapahtua. Tämä on kuin erään-

lainen kantastandardi, koska sitä ei ole spesifioitu minkään tietyn asian suhteen. Siksi sitä voidaankin käyttää erittäin moneen RFID-sovellukseen.

ISO 18000-2 standardi koskee ilmarajapintaparametreja alle 135 kHz:n taajuudella. Se spesifioi fyysisen kerroksen, jota tulee käyttää tietoliikenteessä lukijan ja tunnisteen väillä. Lukijan tulee olla kykenevä lukemaan sekä tyypin A eli FDX(*Full Duplex*) että tyypin B eli HDX (*Half Duplex*) -tunnisteita. Näiden tekniikoiden ero on se, että FDX:ssä informaatiota lähetetään ja vastaanotetaan samaan aikaan ja HDX:ssä eri aikaan. Tyypin A tunnisteet saavat energiansa jatkuvasti päällä olevalta lukijalta. Ne toimivat taajuudella 125 kHz. Tyypin B tunnisteet saavat myös energiansa lukijalta mutta tunnisteen kommunikoidessa lukijan kanssa, on lukija vain kuuntelutilassa. Näin signaali on helpompi napata, koska lukijan paljon vahvempi signaali ei ole päällä häiritsemässä. Toisaalta taas tunniste joutuu lähettämään vain pienten kondensaattorien energialla. Ne toimivat taajuudella 134,2 kHz.

ISO 18000-3 esittelee ilmarajapintaparametrit RFID -järjestelmille, jotka toimivat 13,56 MHz:n taajuudella. Standardi määrittelee kaksi erilaista tapausta erilaisille sovelluksille, jotka eivät ole yhteensopivia. Ne eivät saa missään tapauksissa kuitenkaan häiritä toisiaan.

ISO 18000-4 antaa standardit RFID-teknologialle, joka toimii 2,45 GHz:n ISM (*Industrial, Scientific and Medical*) -taajuuskaistalla. Standardi tukee kaikin puolin ISO/IEC 18000-1 -standardia, ja sen kantomatka on usein yli metrin. Standardi jaetaan kahteen eri osaan tunnisteiden toiminnan mukaan, passiivisiin tunnisteisiin ja ulkoista virtalähdettä käyttäviin tunnisteisiin. Ensimmäinen osa käsittää passiiviset kapeakaistaiset RFID-järjestelmät, jotka pystyvät kommunikoimaan useamman kuin yhden tunnisteen kanssa saman kuulustelualueen sisäpuolella. Toinen osa käsittää pitkän kantaman ja suuren tiedonsiirtonopeuden saavuttavat RFID-järjestelmät. Nopeus saattaa olla jopa 384 kbit/s ilmarajapinnassa R/W (Read-Write) -tunnisteilla. Luettavilla eli R/O (Read-Only) -tunnisteilla nopeus on 76,8 kbit/s.

ISO 18000-5 määrittää standardit 5,8 GHz:n RFID-järjestelmälle. Standardin on tarkoitus spesifioida fyysinen kerros, törmäyksien estäminen ja käytössä oleva protokolla. Tämäkin standardi tukee täysin ISO/IEC 18000-1:stä. Standardi määrittelee erilaisia tapauksia erilaisille sovelluksille, jotka eivät ole yhteensopivia. Nämä eivät kuitenkaan saa häiritä toisiaan.

ISO 18000-6 määrittää standardit RFID -järjestelmille, jotka toimivat 860 - 960 MHz:n taajuusalueella. Standardi määrittää tunnisteen ja lukijan välisen kommunikaation, käytetyt protokollat ja käskyt ja törmäyksien estomääritykset. Lähetyssuuntaan tyyppi A käyttää PIE (*Pulse Interval Encoding*) -koodausta ja tyyppi B käyttää PSK (*Pulse Shift Keying*) -modulaatiota ja *Manchester*-koodausta. Törmäyksien estoon tyyppi A käyttää Aloha-pohjaista menettelyä ja tyyppi B ABT (*Adaptive Binary Tree*) -menettelyä. Paluusuuntaan molemmat käyttävät PSK-modulaatiota ja FM0-koodausta.

ISO 18000-7 -standardin on aikanaan tarkoitus asettaa RFID-järjestelmille määrittelyt, jotka toimivat 433 MHz:n taajuuskaistalla. /2/

3.3.2 ISO 11784-, 11785- ja 14223 -standardit

ISO 11784-, 11785- ja 14223 -standardit käsittelevät eläinten tunnistusta RFID-järjestelmissä. Tunnisteen rakennetta ei ole spesifioitu standardiin, koska vain siten se antaa mahdollisuuden valmistaa juuri oikeanlaisen tunnisteen kullekin eläinlajille. Yleensä tekniikkaa käytetään tunnistamaan lehmiä, lampaita ja hevosia. Steriili lasivaippainen tunniste voidaan asettaa eläimen rasvakudokseen, vaikkapa niskaan, ja siten lukea helposti. RFID-kaulapantoja ja korvatunnisteita on myös käytetty eläimen sisään asetettujen tunnisteiden sijasta. Tällöin ne on myös helppo poistaa jos tarve vaatii.

Tunnistekoodi, jonka tunniste tarjoaa, koostuu kaiken kaikkiaan 64 bitistä. Taulukko 1 esittelee jokaisen bitin tarkoituksen.

Taulukko 1. Tunnistekoodin bittien merkitykset. /1/

Bitti	Merkitys	Kuvaus
1	Eläin (1) tai ei-eläin (0)	Määrittelee sen, että käytetäänkö tunnistetta eläinten tunnistukseen vai ei.
2-5	Varattu	Varattu tulevia sovelluksia varten.
16	data (1) / ei dataa (0)	Kertoo lähetetäänkö lisäinformaatiota tunnistekoodin jälkeen.
17-26	Maakoodi	Kertoo tunnisteen maakooodin, lukujono 999 ilmoittaa tunnisteen olevan testikäytössä.
27-64	Aluekoodi	Maakohtainen rekisterinumero.

Huomionarvoista tunnistekoodissa on se, että bitit 27 - 64 on varattu täysin kohdemaan omaan käyttöön. Niiden käyttöä ei ole mitenkään spesifioitu standardissa. Niitä voidaan käyttää vapaasti määrittämään eläimen tyyppi, rotu, maakunta tai vaikkapa jalostaja.

Standardi määrittää eläinten tunnistukseen kantoaaltotaajuudeksi 134,2 kHz. Käytössä on kaksi eri protokollaa kommunikointiin lukijan ja tunnisteen välillä, Half Duplex- ja Full Duplex -tiedonsiirto.

Half Duplex -kommunikoinnissa käytössä on taajuusmodulaatio FSK (*Frequency Shift Keying*). Tunniste alkaa lähettää välittömästi sen jälkeen kun lukijan lähettämä ”aktivointikenttä” on kytketty pois päältä. Lukija voidaan näin toteuttaa yksinkertaisemmin, koska lukijan ei tarvitse poimia tunnisteen signaalia sen oman aktivointikentän ollessa kytkettynä. Huonompaa tekniikassa on se, että tunniste joutuu lähettämään tunnistekoodin vain pienten kondensaattorien energialla. Loogista nollaa tarkoittaa taajuus 134,2 kHz ja loogista ykköstä 124,2 kHz. Koko siirrettävän datakehyksen koko HDX-kommunikoinnissa on 112 bittiä. Sen lähettämiseen aikaa kuluu maksimissaan 14,5 ms. Tiedonsiirtonopeus vaihtelee 8 387 bit/s (looginen 0) ja 7 762 bit/s (looginen 1) välillä.

Full Duplex -kommunikoinnissa käytössä on amplitudimodulaatio ASK (*Amplitude Shift Keying*). Loogista nollaa vastaa taajuusväli 135,2 - 139,4 kHz ja loogista ykköstä taajuusväli 129,0 - 133,2 kHz. Koko siirrettävän datakehyksen koko FDX-kommunikoinnissa on 128 bittiä. Kehys on 16 bittiä pidempi kuin HDX-kehys, koska *Stuffing* bitti asetetaan joka kahdeksannen bitin väliin. Näin estetään tapaus, jossa lukija voisi luulla uuden kehyksen jo alkaneen vaikka luettaisiinkin vielä vanhaa. Kehyksen lähettämiseen aikaa kuluu maksimissaan 30,5 ms. Tiedonsiirtonopeus on siten 4 194 bit/s.

ISO standardit 11784 ja 11785 eivät ole kuitenkaan täysin virheettömiä. Suurin ongelma lienee siinä, että tunnisteiden valmistajat eivät voi luvata täysin uniikkeja tunnisteita muutoin kuin oman tehtaansa sisällä. Asiaa voitaisiin tarkastella vaikkapa Internetin kannalta. Kaikissa maailman verkkokorteissa on täysin uniikki osoite (tunniste), jota kutsutaan nimellä MAC (*Media Access Control*). Se koostuu 12 heksadesimaalisesta numerosarjasta. Internet ei voisi toimia nykyisellään jos MAC-osoite ei olisi uniikki. Siksi valmistajat pyytävätkin osoitteet ulkopuoliselta taholta, joka pitää huolen siitä, että osoitteet eivät mene sekaisin. Koska ei ole kansainvälistä tahoa, joka jakaisi tunnistekoodeja eläimille, voivat ne mennä helpostikin sekaisin. Tietoturvan taso on täten heikkoa, koska eläimen voisi periaatteessa ”kloonata” vain antamalla sille saman tunnistekoodin kuin on jo käytössä. Esimerkiksi Amazonilta salakuljetettuun papukaijaan voitaisiin asettaa tunniste, joka kertoisi sen olevan Los Angelesin eläintarhasta. Juuri tähän ongelmaan on kehitetty ISO 14223 -standardi. Kuitenkaan ilman kansainvälistä tietokantaa tunnistekoodeista ei eläinten tunnistuksesta voi tulla maailmanlaajuisesti käytössä olevaa järjestelmää. /1,10,11/

3.3.3 ISO 14443 -standardi

Standardi ISO 14443 käsittelee maksu- ja kulkukorteissa käytettyä toteutusta. Biometriset passit on myös usein toteutettu tämän standardin mukaan. Käytetty taajuusalue on 13,56 MHz. Standardi esittelee kaksi eri protokollatyyppiä, joiden toiminta on joiltakin osin poikkeavaa. Molempien protokollien tietoliikenne on määritelty molempiin suuntiin eli lukijasta tunnisteeseen ja toisinpäin. Käytetty termistö tässä standardissa on myös hieman erilainen. Lukijasta käytetään nimitystä PCD (*Proximity Coupling Device*) ja tunnisteesta PICC (*Proximity Integrated Circuit Card*). Lukuetäisyys on verrattain pieni, yleensä se on vain 7 - 15 cm.

Tyypin A kommunikoidessa lukijasta tunnisteeseen bittinopeus on 106 kbit/s. Modulaationa käytetään 100 %:n amplitudimodulaatiota. Koodaus on suoritettu käyttäen *Modified Miller Code* -koodausta.

Tunnisteesta lukijaan kommunikoidessa käytössä on myös amplitudimodulaatio 847 kHz:n (13,56 MHz / 16) alikantoaallolla. Koodaus suoritetaan *Manchester*-koodauksella bittinopeuden ollessa 106 kbit/s (13,56 MHz / 128).

Tyypin B kommunikoidessa lukijasta tunnisteeseen bittinopeus on 106 kbit/s. Modulaationa käytetään 10 %:n amplitudimodulaatiota. Koodaus on suoritettu käyttäen *NRZ* (*No Return to Zero*) -koodausta.

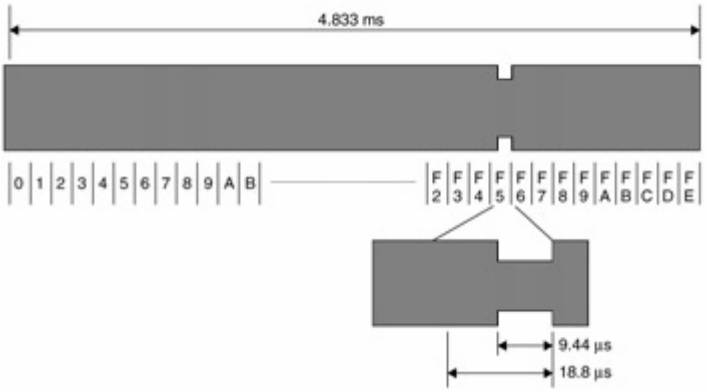
Tunnisteesta lukijaan kommunikoidessa käytössä on vaihemodulaatio 847 kHz:n alikantoaallolla. Koodaus suoritetaan *NRZ*-koodauksella bittinopeuden ollessa 106 kbit/s. /1, 12/

3.3.4 ISO 15693 -standardi

Standardi ISO 15693 käsittelee myös maksu- ja kulkukorteissa käytettyä toteutusta. Erona ISO 14443 -standardiin on se, että lukuetäisyyttä on kasvatettu suuresti. Jopa 1 metrin kantama antaa huomattavasti paremmat edellytykset vaikkapa kulunvalvontasovelluksiin. Käytetty taajuusalue on 13,56 MHz ± 7 kHz.

Tietoliikenne lukijasta tunnisteeseen tapahtuu joko 10 %:n tai 100 %:n amplitudimodulaatiolla. Huolimatta käytetystä modulaatio-indeksistä voidaan valita myös jompikumpi kahdesta koodaustavasta: *1 of 256* -koodaus tai *1 of 4* -koodaus. Standardin mukaan tunnisteen on periaatteessa tuettava molempia koodaus- ja modulaatiotapoja. Kuitenkaan kaikki kombinaatiot eivät ole kovin kannattavia. Käytännössä 10 %:n modulaatiota ja *1 of 256* -koodausta käytetään pitkän matkan sovelluksissa ja 100 %:n modulaatiota ja *1 of 4* -koodausta voidaan käyttää lyhyemmillä kantamilla, tai silloin kun halutaan tarkoituksellisesti lyhyempää kantamaa.

1 of 256 -koodaus käyttää PPM (*Pulse Position Modulation*) tapaa määrittääkseen yksiselitteisesti lähetettävän datan. Riippuen modulaatiopulssin kohdasta, lähetettävä data voidaan määrittää välille 0 - 255. Näin voidaan samalla kertaa lähettää 8 bittiä. Koko tavun lähetysaika on 4,833 ms, bittinopeuden ollessa tällöin 1,65 kbit/s. Aikavälin pituus on 9,44 µs, joten yhteensä niitä mahtuu 4,833 ms ajalle 512 kpl. Modulaatiopulssia ei voida generoida kuin parittomilla aikaväleillä.



Kuva 8. *1 of 256* -koodaus. /1/

1 of 4 -koodaus käyttää myös modulaatiopulssin tiettyä kohtaa hyväkseen määrittääkseen lähetettävän datan. Se voidaan määrittää välille 0 - 3. Kaksi bittiä voidaan siten lähettää kerralla. Modulaatiopulssia ei voida generoida kuin parittomilla aikaväleillä, joten yhden tavun lähettämiseen kuluu aikaa kahdeksan aikaväliä eli 75,52 µs, yhden aikavälin ollessa 9,44 µs. Bittinopeus on tällöin 26,48 kbit/s.

Tietoliikenne tunnisteesta lukijaan tapahtuu joko ASK- tai FSK -modulaatiolla. Se kumpaa käytetään, päättää lukija lähettäessään signaalin tunnisteelle. Lähettävässä signaalissa on varattuna yksi lippubitti tätä toimintoa varten. Kantaman pituuden mukaan voidaan myös bittinopeus valita samoin tavoin joko suuremmaksi tai pienemmäksi. Koodaus tapahtuu käyttäen *Manchester*-koodausta.

Amplitudimodulaatiossa alikantoaallon taajuus on 423,75 kHz. Bittinopeus pitkän kantaman sovelluksissa on 6,62 kbit/s ja lyhyillä kantamilla 26,48 kbit/s.

Taajuusmodulaatiossa alikantoaallon taajuus on 423,75 / 484,28 kHz. Bittinopeus pitkän kantaman sovelluksissa on 6,62 / 6,68 kbit/s ja lyhyillä kantamilla 26,48 / 26,72 kbit/s. /1/

3.3.5 EPC Global G2 -standardi

EPC Generation 2 -standardi on tullut hiljalleen hallitsevaksi standardiksi, etenkin passiivisten UHF RFID -tunnisteiden ja lukijoiden joukossa. Se kehitettiin vuoden 2006 puolivälissä. Standardi keskittyi huomioimaan asiakkaan tarpeet koko toimitusketjun läpi.

Kehitystyöllä oli jo alkuunsa muutamia erittäin ainutlaatuisia piirteitä. Ensiksikin standardia ei suunniteltu jonkin valmistajan teknologian pohjalta ja suunnittelutyöhön otettiin mukaan suuri määrä piiri-, tunniste- ja lukijavalmistajia. Suurin parannus EPC Gen 2 -standardissa olikin juuri se, että tunnisteet voitiin standardisoida yhdeksi, ei moniksi kilpaileviksi standardeiksi. Muilla taajuusalueilla kuin UHF-alueella käytännöt ovat vaihtelevampia mutta suurin kehitys luultavastikin tapahtuu juuri UHF-alueella ja siksi standardille oli jo suuresti kysyntää. EPC Gen 2 -standardista tulee todennäköisesti osa ISO 18000-6 -standardia.

Toinen sukupolvi tarjoaa myös muita etuja kuin edellä mainitut. Se on avoin standardi, joten se on kaikkien käytössä. Laitteet, jotka valmistetaan standardin mukaan, ovat yhteensopivia. Tällöin voidaan periaatteessa kaikkia tunnisteita lukea ilman, että ne häiritsisivät toisiaan. Standardista on myös kehitetty entistä toimivampi, joten lukuvarmuus nousee. Maailmanlaajuinen yhteensopivuus, jota ei aikaisemmin ollut standardisoitu, on myös otettu huomioon. Standardin mukaan tunnisteet voidaan myös sammuttaa lukijalla pysyvästi sekä se mahdollistaa lukijoiden ja tunnisteiden kustannustehokkaan valmistamisen.

EPC-standardi määrittää tunnisteille viisi erilaista luokitusta perustuen niiden ominaisuuksiin. Taulukko 2 esittelee nämä luokat. /2, 13/

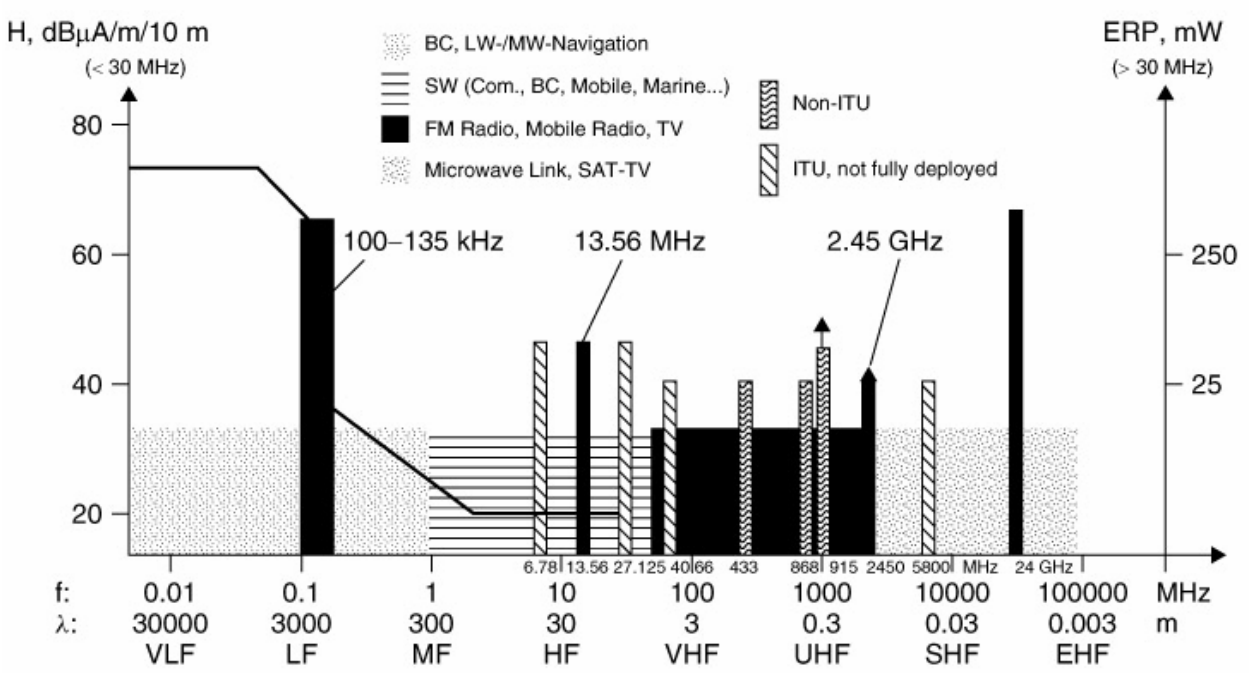
Taulukko 2. EPC Generation 2 -standardin tunnisteluokat. /2/

EPC luokka	Kuvaus	Toiminnallisuus	Huomioita
0	Vain luettava	Passiivinen tunniste	Data voidaan kirjoittaa vain kerran valmistusvaiheessa ja sen jälkeen vain lukea
1	Kerran kirjoitettavissa ja sen jälkeen luettavissa	Passiivinen tunniste	Data voidaan kirjoittaa vain kerran valmistusvaiheessa tai käyttäjän toimesta ja sen jälkeen vain lukea
2	Kirjoitus / luku	Passiivinen tunniste	Käyttäjä voi lukea ja kirjoittaa tunnistetta monesti
3	Kirjoitus / luku	Puoliaktiivinen tunniste	Voidaan varustaa antureilla, jotka keräävät informaatiota esimerkiksi lämpötilasta ja/tai paineesta
4	Kirjoitus / luku	Aktiivinen tunniste	Voidaan varustaa antureilla ja toimii radiolähettimenä kommunikoidakseen lukijan kanssa

3.4 Käytössä olevat taajuudet RFID-teknologiassa

Taajuusalueet eivät ole kovinkaan hyvin standardisoituja RFID-teknologiassa, paitsi EPC Gen 2 -standardissa määrätyillä UHF-alueilla. Vaikka periaatteessa taajuuksien käyttö on jokaisen maan päätettävissä, jonkinlainen yhdenmukaisuus taajuuksien käytössä on luonnollisesti järkevää. Tästä syystä muutamat taajuudet ovat vakiinnuttaneet paikkansa juuri RFID-taajuuksina. Ei olisi lainkaan suotavaa, että RFID-taajuudet menisivät päällekkäin esimerkiksi GSM-järjestelmän tai lennonjohdon kanssa.

Käytössä olevat taajuusalueet RFID-teknologiassa voidaan jakaa karkeasti neljään eri alueeseen, joissa muutamissa on eroa riippuen maasta. Kuvassa 9 on esitettynä taajuusalueet eri järjestelmissä.



Kuva 9. Käytössä olevat RFID -taajuudet. /1/

3.4.1 LF (*Low Frequency*) -taajuusalue

LF-taajuusalue määrittyy alle 135 kHz:n taajuuksiin. Näistä taajuuksista käytetyimpiä ovat 125 kHz:n ja 134 kHz:n taajuudet. Tunnisteet ovat tyypillisesti passiivisia ja vaativat kalliimman ja pidemmän antennin toimiakseen. Selkeänä etuna voidaan pitää sitä, että tämä taajuusalue on kaikkein vähiten herkkä metallille ja nesteille. Haittapuolena on taas pienempi lukuetäisyys, hitaampi tiedonsiirtonopeus ja suurempi tunnistekoko kuin muilla taajuuksilla.

Käyttösovelluksia LF-alueella ovat lähinnä eläinten seuranta, kulunvalvonta, autotekniikka, sairaanhoito- ja POS (*Point of Sale*) -sovellukset. Mobil/Exxon on tuonut markkinoille POS-tunnisteen, jossa avaimenperällä (RFID-tunniste) voidaan ostaa polttoainetta. Tämä järjestelmä on erittäin suosittu moottoripyöräilijöiden keskuudessa Yhdysvalloissa. /14,15/

3.4.2 HF (*High Frequency*) -taajuusalue

HF-taajuusalue käsitetään yleensä 13,56 MHz taajuutena. Tämä alue tarjoaa käytössä suuremman kantaman ja nopeamman tiedonsiirtonopeuden LF-sovellukset. Tunnisteet ovat tyypillisesti passiivisia tällä alueella. Hinnaltaan HF-tunnisteet ovat tyypillisesti edullisempia kuin muut tunnisteet. HF-tunnisteiden luettavuus veden tai metallien läheisyydestä ei ole niin hyvä kuin LF-tunnisteilla mutta kuitenkin parempi kuin UHF-tunnisteilla.

Sovelluskohteita 13,56 MHz:n alueella ovat luottokortit ja ”älykkäät hyllyt”, jotka huolehtivat tavaroiden inventaariosta. Käytössä on myös sovelluksia, jossa seurataan kirjaston kirjoja ja sairaaloiden potilaita. Tuotteita ja lentolaukkuja voidaan tunnistaa tällä järjestelmällä. Tunnisteet voivat myös tarjota informaatiota säännöllisesti huoltoa vaativista laitteista kuten palonsammutusjärjestelmistä. /14,15/

3.4.3 UHF (*Ultra-High Frequency*) -taajuusalue

UHF-taajuusalueella tarkoitetaan 868 MHZ - 956 MHz välistä aluetta. Tyypillisesti Euroopassa se on 868 MHz, Yhdysvalloissa 915 MHz ja Japanissa 950 - 956 MHz. UHF-tekniikka tarjoaa suuremman tiedonsiirtonopeuden ja kantaman kuin HF-tekniikka, mutta tunnisteet maksavat suurin piirtein saman verran. Tunnistetyyppi UHF-alueella voi olla passiivinen tai aktiivinen, riippuen täysin sovelluskohteesta.

Taajuusalue tarjoaa hyvän läpäisykyvyn ei-johtavien materiaalien ja nesteiden osalta. Se toimii myös erittäin hyvin tilanteissa, jossa joudutaan lukemaan useita tunnisteita samanaikaisesti. RFID-järjestelmien kehitys on suurinta juuri tällä alueella nykypäivänä, eikä vähiten juuri EPC Global -standardien vuoksi, jotka ovat tehneet yhtenevät järjestelmät mahdollisiksi.

Huonot puolet UHF-tekniikassa tulevat esille varsinkin silloin kun joudutaan olemaan tekemisissä metallien ja johtavien nesteiden kanssa. Tunniste, joka on asen-

nettu suoraan metalliseen kappaleeseen, voi jopa jäädä kokonaan lukematta, koska radioaalto ei voi läpäistä kappaletta. /14,15/

3.4.4 Mikroaaltotaajuusalue

Neljäs ja viimeinen vaihtoehto RFID-järjestelmille on mikroaalto taajuusalue, joka on joko 2,45 GHz tai 5,8 GHz. Tunnisteilla on hyvin samanlaiset ominaisuudet kuin UHF-tunnisteilla mutta maksavat yleensä kaksi kertaa enemmän. Tiedonsiirtonopeus on suurempi mutta kantama on rajoittuneempi kuin UHF-alueella.

Metallit ja johtavat nesteet saavat mikroaallot heijastumaan, joten tämä taajuusalue ei käy ollenkaan käytettäväksi niiden läheisyydessä. Siksi mikroaalto RFID-sovellukset ovatkin yleensä käytössä juuri niille räätälöidyissä paikoissa, kuten lentolaukkujen tunnistuksessa.

Toisaalta suuri tiedonsiirtonopeus houkuttelisi käyttämään mikroaaltotekniikkaa myös logistiikassa. Tosiasiassa tekniikan rajoittuneisuus läpäistä metallia sulkee tämän vaihtoehdon pois käytännössä kokonaan. Lukuvarmuus jäisi varmasti alle toivotun tason ja tekniikasta olisi näin ollen enemmän haittaa kuin hyötyä. /14,15/

3.5 Muistit

Monetkaan RFID-tunnisteet eivät vaadi kovin mittavaa muistikapasiteettia. Yksinkertaisen tuotekoodin säilyttäminen tunnisteessa ei vie paljon tilaa. Kuitenkin järjestelmät, jossa on käytössä erialaisia sensoreita esimerkiksi lämpötilan- tai liikkeiden tarkkailuun, tarvitsevat huomattavasti enemmän muistia. Ne tarvitsevat myös kirjoitusmahdollisuuden datan keräystä varten. Karkeasti voidaankin jakaa RFID-teknologiassa käytetyt muistit niiden ominaisuuksien mukaan: lukumahdollisuuden tarjoavat muistit, ohjelmoitavat muistit ja luku- sekä kirjoitusmahdollisuuden tarjoavat muistit.

Lukumahdollisuuden tarjoavia R/O-muisteja ei voida kirjoittaa enää uudelleen. Niihin kirjoitetaan valmistusprosessissa tietty tunnistekoodi, joka pysyy samana koko tunnisteen elinkaaren ajan. Yleensä muistin koko on hyvin pieni ja siksi tämän tyyppiset tunnisteet ovatkin verrattain halpoja toisiin muistityyppeihin nähden.

WORM (*Write Once Read Many*) -muistit mahdollistavat kirjoituksen kerran ja sen jälkeen niitä voidaan vain lukea. Kaikkiin WORM-muisteihin ei ole kuitenkaan mahdollista kirjoittaa koko muistialueelle, vaan vain pieneen osaan muistialueesta voidaan vaikuttaa. Tämän tyyppiset muistit ovat erittäin hyödyllisiä asiakkaille, joilla on paljon erialaisia tarpeita. Näin voidaan hankkia vain yhtä muistityyppiä sisältäviä tunnisteita ja ohjelmoida ne omien tarpeiden mukaisesti.

Luku- ja kirjoitusmahdollisuuden tarjoamaan R/W-muistiin voidaan kirjoittaa samalla kun tunnistetta luetaan lukijalla. Nämä ovat luonnollisesti kalleimpia muisteja. Tyypillisesti nämä ovat EEPROM (*Electrically-Erasable Programmable Read-Only Memory*) tyyppisiä NVRAM (*non-volatile RAM*) -muisteja, jotka säilyttävät datan vaikka tunnisteessa ei olisikaan virtalähdettä. Koko muisti voidaan näin halutessa tuhota ja kirjoittaa uudestaan sähköisesti. /4,5/

4 RFID-sovelluksia

RFID-teknologiaa voidaan käyttää melkein joka paikassa missä viivakoodejakin. Sillä on kuitenkin huomattavasti enemmän ominaisuuksia kuin viivakoodeihin perustuvalla tunnistuksella. Ensiksikin yleensä ei ole merkitystä mihin tunniste on sijoitettu. Se voi olla näkyvissä tai ei, toisin kuin viivakoodit.

Tunnisteet ovat myös kestäviä likaa, kuumuutta, maaleja, liottimia ja muita tunnisteita vastaan. Tämä antaa niille huomattavan edun paperisiin viivakoodeihin nähden, jotka voidaan poistaa tai repiä kuljetuksessa. Ne voivat myös helposti likaantua niin paljon, että tuotteen tunnistaminen on mahdotonta.

Kuten jo aikaisemmin tässä työssä muisteja käsittelevässä luvussa mainittiin, tunnisteet voivat myös säilöä tietoja. Tähän eivät viivakoodit pysty. Tämä, mukaan luettuna sovellusten suuri kantama, antaa RFID-sovelluksille huomattavasti enemmän käyttökohteita kuin viivakoodeille.

Kuten kaikilla teknologioilla, myös RFID:llä on omat haittapuolensa. Tunnisteiden on oltava järkevän hintaisia, muutoin yksikään valmistaja ei ala käyttää niitä. Kärjistetysti sanottuna 80 sentin maitotölkkiin ei asenneta 10 sentin tunnistetta. Yksityisyys- ja turvallisuusasiat ovat myös seikkoja, jotka askarruttavat kuluttajia ja valmistajia. Kaikkiin näihin kysymyksiin on oltava vastaukset ennen kuin teknologia yleistyisi vielä siitä mitä se on tänä päivänä.

Sovellukset voidaan jakaa niiden kantaman mukaan kahteen eri kategoriaan, lyhyen- ja pitkän kantaman sovelluksiin.

4.1 Lyhyen kantaman RFID-sovellukset

Lyhyen kantaman sovellukset ovat nimensä mukaisesti sellaisia, että lukijan ja tunnisteen välinen etäisyys on hyvin pieni. Yleensä kantama on alle 30 cm. Tunniste voi tässä tapauksessa olla kortti tai ranneke, joka asetetaan käyttäjän toimesta lähelle lukijaa.

Kulunvalvonta on tyypillinen esimerkki lyhyen kantaman RFID-sovelluksesta. Siinä yleensä kortti tai muu kulkulupa asetetaan lähelle lukijaa, joka sitten ilmoittaa vaikkapa valolla ja/tai äänellä pääsystä tai sen hylkäyksestä. Tekniikka ei sinänsä ole uusi, magneettiraidalliset kortithan ovat olleet jo pitkään käytössä kulunvalvonnassa. RFID tuo kuitenkin aivan uusia mahdollisuuksia kulunvalvontaan ja etenkin sen hallittavuuteen. Esimerkiksi henkilön poistuminen laboratoriossa voidaan estää jos hän ei ole käynyt ensiksi puhdistautumassa. Lukijat tietävät, että onko henkilö avannut puhdistushuoneen oven ja jos näin ei ole, niin kulku pois laboratoriosta hylätään. RFID-tunnisteet ovat myös turvallisia, koska niitä ei voi muokata. Toisin on magneettiraidallisten kulkulupien, joiden tieto voidaan tuhota ja kirjoittaa uudelleen. Koska lukijat eivät tarvitse fyysistä kosketusta tunnisteen kanssa, on myös huollon tarve tällöin minimaalinen. Federal Express käyttää joissakin ajoneuvoissa myös tavaratilaan pääsyn hallintaan RFID-rannekkeita. Hallituksen rakennuksissa, pääasiassa Yhdysvalloissa, on myös kulkuluvan lisäksi vaadittu verkkokalvotunnistus, joka edelleen lisää turvallisuutta. /4/

Julkisen liikenteen lipuissa RFID:tä on käytetty jo pitkään myös Tampereella. On erittäin helppoa niin asiakkaalle kuin liikennelaitoksellekin, että kaikilla on sama lippu, johon voi sitten halutessaan ladata erilaisia matkoja. Samantyyppiset tunnisteet, vaikkapa ranteisiin menevät, sopivat ideaalisesti myös huvipuistoihin tai konsertteihin. Ne ovat kohtuullisen halpoja ja niistä voidaan tehdä kertakäyttöisiä. Merkittävä etu saavutetaan myös sillä, että RFID-tunnistetta ei voi väärentää. Paperisen pääsylipun saattaa voida väärentää melko helpostikin, varsinkin jos sen autentikointi jää vain ovella seisovan ihmisen tehtäväksi. Lukijaa ei kuitenkaan voi huijata ja näin poistuu myös inhimillisen erehdyksen vaara. /4/

Turvallisuuden lisääminen on ollut jo muutaman vuoden tekniikan kannalta eteenpäin vievä voima, ja näin on käynyt myös RFID-teknologiassa. Henkilöiden valvontaan tämä tekniikka sopii erittäin hyvin. Kun tunnisteeseen koodataan tietyn henkilön tunnistuskoodi, voidaan tätä seurata kaikkialla rakennuksen sisällä reaaliajassa. Näin voidaan vaikkapa varmistaa, että vartijat partioivat aina heille kuuluvan alueen. Toisaalta vangeille voidaan laittaa rannekkeet, jotka toimivat 13,56 MHz:n taajuudella. Aina kun vanki kulkee lukijan lävitse, tallentuu hänen liikkeensä tietokantaan. Tunnisteesta voidaan vanki myös tunnistaa koska tahansa ja siihen voidaan koodata vangin ”päiväraha”, jonka hän voi kuluttaa kanttiinissa. Armeija käyttää RFID-tunnisteita, jotka ovat napin kokoisia ja ommeltuina sotilaiden vaatteisiin. Niistä voidaan hetkessä lukea sotilaan nimi, veriryhmä, lääkeallergiat, yksikkö, sotilasarvo ja kaikkea muuta mikä vain voisi olla hyödyllistä sodankäynnissä. /4/

Sairaanhoidossa on myös havaittu RFID:n mahdollisuudet. Koska tällä sektorilla virheisiin ei ole varaa, voidaan potilaat, veri ja elimet tunnistaa luotettavasti RFID:llä. Näyteputkiin voidaan asentaa tunnisteet, joista voidaan sitten myöhemmin lukea missä näytteet on kerätty, missä ne ovat olleet keräämisen jälkeen ja missä ne ovat analysoitu. /4/

Erittäin haitalliset ongelmajätteet ovat hyvin tarkkaan kontrolloituja niiden varastoinnin, tunnistuksen, käsittelyn ja lopullisen hävityksen osalta. Silloin tavalliset viivakoodit voivat liiankin helposti repeytyä tai tuhriintua käyttökelvottomiksi, jota ei tietenkään voi hyväksyä näinkin kriittisissä materiaaleissa. Näin ollen RFID tarjoaa helpon tavan tunnistaa materiaalit luotettavasti. /4/

RFID on edennyt myös ajoneuvojen tunnistukseen lyhyenkin kantaman sovelluksissa. Vuokraliikkeet voivat esimerkiksi laittaa tunnistimet autoihinsa, jotta he tietävät tarkalleen mihin auto on parkkipaikalla pysäköity. Näin voidaan asiakasta palvella nopeasti kun inventaario on aina ajan tasalla. Toisaalta ajoneuvoihin asennettuja tunnisteita voidaan käyttää myös kulunvalvontaan. Taloyhtiö voi jakaa kaikille asukkaille tunnisteet asennettaviksi ajoneuvoihin. Näin aina kun tunniste tulee

riittävän lähelle autotallin porttia, se aukeaa ilman asukkaan ylimääräisiä toimia. Tällä tavoin ei tarvittaisi mitään ylimääräisiä kaukosäätimiä tai avaimia. /4/

EU:n jäsenmaissa on jo valmistettu passeja, joissa on RFID-tunniste kanteen integroituna. Tämä johtuu pitkälti Yhdysvaltojen vaatimuksesta, että matkustajien passeissa tulisi olla tunnisteet. Passeihin voidaan tällöin tallentaa henkilön sormenjäljet, valokuva, passin tietoja ja muuta tarpeellista. /4/

4..2 Pitkän kantaman RFID-sovellukset

Pitkän, tai ainakin pidemmän, kantaman sovellukset käyttävät usein aktiivisia tunnisteita, koska niiden täytyy lähettää informaatiota pidempiä matkoja. BAP-tunnisteet ovat myös mahdollisia pitkän kantaman sovelluksiin.

Tuotantoketjussa riman on asettanut hyvin pitkälti yksi yhtiö, yhdysvaltalainen maailman isoin yhtiö Wal-Mart. Se antoi vuonna 2003 määräyksen toimittajilleen, että kaikissa heidän toimittamissaan tuotteissa pitää olla RFID-tunniste niiden seurannan helpottamiseksi. Kaikki ne toimittajat, jotka eivät voisi täyttää näitä ”toiveita”, tultaisiin käsittelemään toisarvoisina. Tämä sai tavarantoimittajat liikkeelle erittäin tosissaan. Tavarantoimittajille ensimmäinen ongelma oli kuitenkin se kaikkien ilmeisin. Silloin tunniste maksoi noin 0,05 $ kappaleelta. Yhtiöille, jotka toimittavat miljoonia tuotteita vuosittain Wal-Martille, tämä oli liikaa. Siksi myös Wal-Mart muutti määräyksiään ja myöntyi siihen, että vain kuormalavoissa oli oltava tunnisteet. Kaiken kaikkiaan tämä tarkoitti sitä, että vuonna 2004 valmistajaa kohti lisäbudjettia RFID-hankkeeseen vaadittiin 13 - 23 miljoonaa dollaria. Tämän ajateltiin kuitenkin joskus tulevaisuudessa johtavan siihen, että tavarataloissa voitaisiin taata tuotteiden saatavuus 100 %:n varmuudella silloisen 99,3 %:n sijasta. Luvut eivät sinänsä vaikuta suurilta, mutta kun on kyse Wal-Martista, niin ero suhteutettuna liikevaihtoon olisi noin miljardi dollaria. /4/

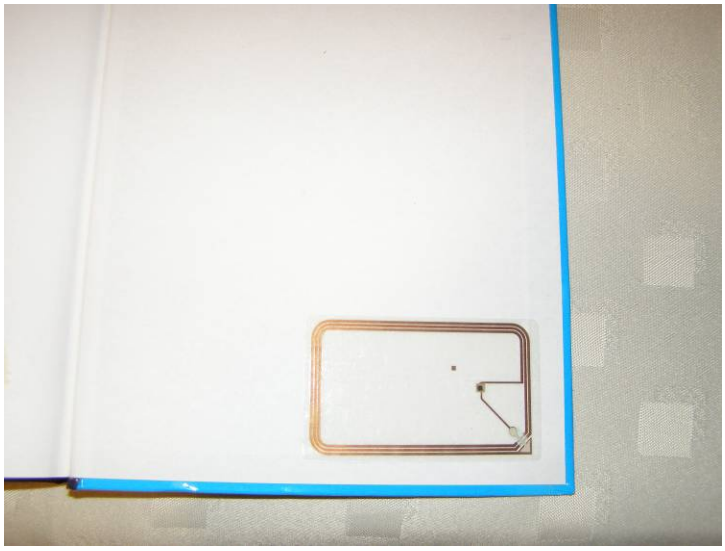
Kuljetusyrityksissä ja postilaitoksissa paketteihin on jo esimerkiksi Ruotsissa asennettu RFID-tunnisteita. Jos paketti avataan kuljetuksen aikana, tallentuu siitä tiedot tunnisteeseen. Näin tiedetään varmuudella, että joku on peukaloinut pakettia ja sisältöön tarvitsee suhtautua varauksella. Isoihin merikontteihin voidaan asentaa tunnisteet, jotka hälyttävät välittömästi vaikkapa laivan palvelimelle jos kontti avataan kuljetuksen aikana. Tunnisteet kykenevät myös tallentamaan olosuhteet, jolloin paketit avattiin. Esimerkiksi liiketunnistimilla voidaan tarkastella avautuiko paketti mahdollisesti pudotuksen seurauksesta ja lämpötila-antureilla saadaan tarkka lämpötilalukema tallennettua. /4/

Maailman kauppajärjestö WTO (*World Trade Organization*) on ollut hyvin kiinnostunut RFID-tekniikasta, jolla pystytään tunnistamaan ja autentikoimaan tuote. Tämän tyyppiset sovellukset ovat kohdistuneet lähinnä vaatteisiin. Niihin voidaan ommella vaikkapa pesulappuun pieni tunniste, joka pystyy lähettämään oman tunnistekoodinsa ja siten voidaan varmuudella sanoa vaatekappaleen olevan aito. /4/

Lentoyhtiöt ovat järjestäneet testejä koskien matkalaukkuihin asennettavia RFID-tunnisteita. Kuva 10 osoittaa tavan, jolla laukut merkataan. Jokaiseen laukkuun, joka on menossa lentokoneen ruumaan, liimataan kuvan mukainen tarra avain kuten aikaisemminkin. Ainoa ero on se, että testeissä tarrassa oli tunniste viivakoodin lisäksi. Lentolaukkujen käsittely ei varsinaisesti aina ole hellävaraista lentokentillä, joissa matkaa kymmeniä tuhansia ihmisiä päivittäin. Tästä syystä viivakooditkin menevät usein sellaisiksi, että lukija ei pysty sitä käsittelemään. Testeissä RFID-tunnisteilla pystyttiin nostamaan lukuvarmuutta 90 prosentista 99 prosenttiin. On arvioitu, että kaikista 3 miljardista matkalaukusta 1 % ei päädy oikeaan kohteeseen. Se tarkoittaa, että noin 30 miljoonaa matkalaukkua hukataan joka vuosi. RFID:llä voitaisiin tuotakin lukemaa huomattavasti pienentää ja samalla säästää lentoyhtiön kuluja. Luku- ja kirjoitusominaisuudella varustettuihin tunnisteisiin voitaisiin matkan varrella myös kirjoittaa vaikkapa turvallisuustarkastuksen suorittaneen lentokenttävirkailijan nimi. /4,16/

Kuva 10. RFID matkalaukuissa. /16/

Monet kirjastot käyttävät nykyisin RFID:tä automatisoimaan kirjojen, CD- ja DVD -levyjen ja nauhojen palautusta. Näin voidaan rakentaa kirjastoon myös erittäin luotettava ja reaaliaikainen inventaariosysteemi. Hyllyihin asennettavat lukijalaitteet havaitsevat kirjat ja tallentavat ne tietokantaan. Tunniste kirjoihin ja muihin tuotteisiin on erittäin helppo asentaa, koska se voidaan yksinkertaisesti liimata kanteen. Kuva 11 esittää ToP Tunniste Oy:n *RFID Handbook* kirjan kannessa olevan tunnisteen. Ennen RFID:tä kaikki materiaali, joka lainattiin kirjastosta, lainattiin viivakoodeja käyttämällä. Tämä tarkoitti sitä, että kirjat ja muu materiaali jouduttiin käyttämään viivakoodilukijassa yksi kerrallaan juuri oikein päin. Tätä varten oli pakko palkata oma virkailijansa, jonka tehtävänä oli valvoa, että kaikki lainattava materiaali tuli luetuksi järjestelmään. Nykyisin asiakas voi itse vain yksinkertaisesti asettaa kaikki lainattavat materiaalit lukijan läheisyyteen ja kaikki voidaan lukea kerralla. Täten toiminta nopeutuu, ja mikä tärkeintä, henkilökuntaa ei tarvita lainkaan.



Kuva 11. RFID-tarratunniste kirjan kannessa. /19/

Ruoan tuonti ulkomailta sekä maan sisäinen liikenne todennäköisesti kasvaa tulevaisuudessa. Siksi on tärkeää tietää mistä se on peräisin. Esimerkiksi Yhdysvalloissa sattuneessa tapauksessa, jossa lehmän todettiin sairastavan BSE:tä (hullun lehmän tautia), oli erittäin vaikeaa saada selville mistä lehmä oli alkujansa kotoisin. Yksi ratkaisu, kuten jo aikaisemmin tässä työssä on mainittu, on asettaa eläimen rasvakudokseen lasivaippainen RFID-tunniste. Kuvassa 12 on muutama esimerkki tämän tyyppisistä tunnisteista. Pienempiä tunnisteita voidaan käyttää kotieläimillä. Yhdysvalloissa odotetaankin, että pian tulee voimaan laki, joka pakottaa kasvattajat asettamaan karjaansa sähköiset tunnisteet.

Kuva 12. Lasivaippainen RFID-tunniste. /17/

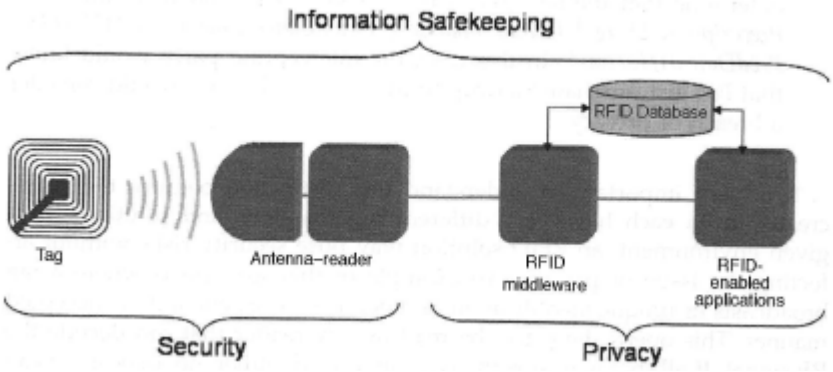
5 Informaation turvaaminen RFID-teknologiassa

Puhuttaessa informaation turvaamisesta (*Information Safekeeping*) RFID-teknologiassa, käsite ei ole aivan yksiselitteinen. Käsite voidaan jakaa kahteen osaan, tietoturvaan (*Security*) ja yksityisyyteen (*Privacy*).

Tietoturva tässä yhteydessä voitaisiin ajatella kyvyksi pitämään *data* tunnisteen ja lukijan välillä vain niiden välisenä, suojassa muilta vastaanottajilta. Tietoturvamurtona voitaisiin ajatella sellaista tilannetta, että jokin kolmas osapuoli saisi vastaanotettua viestin tunnisteen TRG152 ja lukijan LJ välillä. Kolmas osapuoli voisi myös lukea viestin sisällön ”XYZP52OK”. Kuitenkaan tästä ei voitaisi päätellä mitä tämä viesti tarkoittaa.

Yksityisyys tarkoittaa tässä tapauksessa sitä, että voidaan pitää *viestin tarkoitus* turvattuna tunnisteen ja lukijan välillä. Esimerkiksi jos kolmas osapuoli vastaanottaisi jo aikaisemmin esitetyn viestin ”XYZP52OK” tunnisteen TRG152 ja lukijan LJ välillä vaikkapa ostoskeskuksessa. Tästä hän voisi myös päätellä viestin tarkoittavan seuraavaa: ”Tuote: Warsteiner | Luokka: Mallasolut | Viimeinen myyntipäivä: 060608”. Nyt olisi saatu selville, että asiakas osti juuri olutta ja tätä voitaisiin pitää yksityisyysmurtona.

RFID-ympäristöt ovat erilaisia ja siksi näihin kahteen ongelmaan on myös erilaisia ratkaisuja. Voi olla mahdollista, että tietoturvariski on olemassa mutta se ei kuitenkaan aiheuta yksityisyyteen liittyvää riskiä. Ajatellaan vaikkapa tunnistetta, joka lähettää täysin luettavissa olevaa omaa tunnistekoodiansa. Tämä koodi on luettavissa kaikilla sopivilla lukijoilla. Ilman pääsyä tietokantaan (*RFID Database,* kuva 13), ei itse tunnistekoodista ole kenellekään suoraa hyötyä. Se ei kuitenkaan poista mahdollisia ongelmia, jotka koskevat *luettelointia* ja *jäljitettävyyttä.* /5/



Kuva 13. Informaation turvaaminen ja sen eri merkitykset. /5/

5.1 Luettelointi ja jäljitettävyys

Luettelointi ja jäljitettävyys ovat käsitteitä, jotka liittyvät tilanteeseen, jossa jokin kolmas osapuoli lukee luvatta tunnisteen tarjoaman koodin. Koodia lukiessa ei välttämättä olla lainkaan kiinnostuneita siitä, missä tavarassa tunniste on kiinni tai kuka sitä kantaa. Toisin sanoen, vain lukemalla RFID-signaalin, voidaan jäljittää missä tunniste on tai on ollut ja luetteloida kaikki havaitut tunnisteet.

Jäljitettävyyttä voidaan hyvin kuvailla seuraavalla esimerkillä. Kuluttaja ostaa vaatekaupasta neuleen, käsilaukun ja kengät. Kaikissa näissä tuotteissa on passiiviset RFID-tunnisteet asennettuina. Kun kuluttaja lähtee kaupasta, kuka tahansa jolla on sopiva laite voi lukea tunnisteiden sisällön. Vaikka tunnisteen lähettämä koodi olisikin kryptattu, se on silti yksilöllinen ja toistettavissa. Tämä tarkoittaa sitä, että niin kauan kuin tämä signaali voidaan lukea, niin tiedetään, että seurataan juuri esimerkin kuluttajaa. Kuluttajan saapuessa samaan kauppaan kuukauden kuluttua samoilla kengillä, jotka hän osti viimeksi siellä asioidessaan, voidaan paikalle hälyttää myyjä esittelemään samantyyppisiä tuotteita. Monet ihmiset pitäisivät heidän yksityisyyttään loukattuna tällaisesta toiminnasta.

Luettelointi on ehkäpä vielä suurempi kysymysmerkki koskien toisen henkilön yksityisyyttä. Se tarkoittaa sitä, että kuluttajan ostaessa tuotteita, jotka on varustettu EPC-tunnisteilla, voidaan ne lukea sopivalla lukijalla. Esimerkiksi työnantaja voisi

työntekijän tullessa töihin lukea hänen käsilaukkunsa sisällön. Jos työntekijällä sattuisikin olemaan vaikkapa mielialalääkkeitä laukussaan, voisi työnantajan ja työntekijän keskinäinen suhde vaarantua.

Kuten jo aikaisemmin tässä työssä on käsitelty, pitkälti Yhdysvaltojen vaikutuksesta myös EU-passeihin on lisätty RFID-tunnisteet. Alun perin suunnitelmissa ei ollut salata passien tietoja mitenkään. Kuitenkin terroristien ja muiden väärinkäytösten pelossa lisättiin passeihin myös tietoturvaa. Ensiksikin kaikki tieto passissa on kryptattua. Toiseksi avain, jolla informaatio saadaan avatuksi, on koodattu passiin ja voidaan lukea vain optisella lukijalla. Kolmanneksi passien kannet on vuorattu metallilla, jotta ne muodostaisivat Faradayn häkin. Näin passia on teoriassa mahdotonta lukea kun kannet olisi suljettuina. Nämä menettelyt tietoturvan parantamiseksi eivät kuitenkaan ole saaneet kaikkia alan eksperttejä vakuuttuneiksi. Muutamat tahot väittävät, että vaikka passien sisältämä tieto olisikin kryptattu, voisi passeja silti jäljittää. Passissa oleva tunniste lähettää kuitenkin yksilöllisen tunnistekoodin, joka voidaan yhdistää tiettyyn henkilöön vaikka varsinaista tietoa ei voitaisikaan lukea. /5/

5.2 Tietoturva

Alun perin kaupallisissa RFID-sovelluksissa ei ajateltu tietoturvaan liittyviä asioita. Tunnisteet ja lukijat kommunikoivat täysin avoimesti ilman minkäänlaista kryptausta. Myös nykypäivänä useimmissa sovelluksissa kommunikoidaan avoimesti. Tämä johtuu suuresti siitä, että tunnisteista yritetään tehdä mahdollisimman halpoja. Näin ne on suunniteltu siten, että niissä on vain hyvin rajallinen prosessointikyky. Siten on erittäin vaikeaa käyttää salausalgoritmeja muuta tekniikkaa tunnisteissa.

RFID-teknologiassa on turvallisuusuhkia, joita vastaan suurempaan tietoturvaan tähtäävien sovellusten olisi hyvä suojautua. Tässä kappaleessa näistä uhkista esitellään muutamat tunnetuimmat.

Tunnisteiden salakuuntelu (*Eavesdropping*) tarkoittaa sitä, että jokin kolmas osapuoli kuuntelee tunnisteiden lähettämää dataa. Koska RFID:n perusidea on se, että tunnisteet lähettävät dataa lukijalle, voidaan tällainen toiminta suorittaa usein täysin huomaamatta.

Huijaus (*Spoofing*) tarkoittaa sitä, että jos tekniikan käyttämät turvallisuusprotokollat saadaan selville, voidaan kirjoittaa itse tunnisteita. Esimerkiksi supermarketeissa voitaisiin tunnisteen sisältämä data kirjoittaa uudelleen, jotta saataisiin tuote kassalla halvemmalla.

Kloonaus (*Cloning*) tarkoittaa tilannetta, jossa jonkin tunnisteen lähettämä signaali tallennetaan. Laitteet, jotka tallentavat signaalin, kykenevät myös lähettämään sen uudestaan tarvittaessa. Näin esimerkiksi automatisoituja tietullijärjestelmiä voitaisiin huijata siten, että lähetettäisiin täysin toisen auton signaalia. Siten vältyttäisiin tyystin tietullimaksuilta. /5/

5.3 Suojattu RFID-ympäristö

Useita ehdotuksia on esitetty vastaamaan kysymykseen siitä, että miten voitaisiin luoda suojattu RFID-ympäristö tunnettuja uhkia vastaan. Muutamia käytössä olevia menetelmiä esitellään tässä kappaleessa.

Faradayn häkki on melko karkea menetelmä lisäämään tietoturvaa. Menetelmä perustuu siihen, että kotelot jotka ovat tehty tietyistä metalleista ja joilla on tietty muoto, muodostavat luonnollisen suojan radioaaltoja vastaan. Periaatteessa tämä on myös ehkäpä yksi suurimmista ongelmista RFID-teknologiassa. Tässä tapauksessa tätä ongelmaa käytetään hyväksi. Jotta tämä menetelmä olisi tehokas, pitäisi henkilön avata tunnisteen kotelo jokainen kerta kun hän haluaisi tunnisteen toimi-

van. Tunnisteen ollessa ulkona kotelosta, olisi se tietenkin täysin vailla suojaa. Vaikkakin tämä tapa ei ole kovinkaan kehittynyt, tarjoaa se jonkinlaisen suojan uhkia vastaan tietyissä sovelluksissa. Kuten jo aikaisemmin tässä työssä on esitetty, on passien kansiin rakennettu Faradayn häkkiin perustuva tietoturvaratkaisu. Salausavain, joka voidaan lukea vain optisesti, turvaa passien tietoja tietysti lisää. Tässä tapauksessa tämä ratkaisu toimii kohtalaisen hyvin, koska yleensähän passin kannet ovat kiinni paitsi silloin kun niitä pitäisi esittää virkailijalle.

Toinen tapa suojata järjestelmää, käyttää hyväkseen myös yhtä tunnettua radiosignaalin heikkoutta. RF-signaali vaimenee aina väliaineessa. Tästä syystä tunniste voidaankin suunnitella siten, että sen lähettämä signaali on luettavissa vain muutamien senttimetrien päästä. Tämä suojaustapa ei kuitenkaan ole kovinkaan tehokas. Ajatellaanpa vaikka eräänlaista RFID-maksukorttia Tokion metrossa ruuhka-aikaan. On käytännössä täysin mahdotonta sijoittaa itsensä siten, että kukaan ei olisi hyvinkin lähellä. Kuitenkin rakennuksissa, joiden ympäristöt ovat tarkoin vartioituja, voidaan käyttää rajoitetun kantomatkan tunnisteita ja saavuttaa pelkästään siten kohtalaisen turvattu järjestelmä.

Tunniste on myös mahdollista sammuttaa kokonaan (*Kill*). Silloin se ei ole enää koskaan käyttökelpoinen. Sammutuskäsky on sisäänrakennettu sitä tukeviin tunnisteisiin. Käsky voidaan suorittaa vaikkapa tuotteen ostopaikalla siten, että lähetetään tunnisteelle tietty koodi, joka sammuttaa sen. Vaikkakin tämä menettely on erittäin tehokas, siinä on silti muutamia merkittäviä haittapuolia. Ensiksikin se ei tarjoa mitään suojaa uhkia vastaan ennen käskyn suorittamista. Siksi tarvitaankin muita tapoja suojaamaan tunnisteen sisältämää informaatiota sen elinkaaren ajaksi. Toiseksi se estää tunnisteen käytön tulevaisuudessa joissain toisissa sovelluksissa. Esimerkin valossa voidaan käsitellä vaatekappaleisiin asennettuja tunnisteita ja niitä lukevia kodinkoneita. Esimerkin valossa voidaan tutkia asiakasta X, joka on juuri ostanut RFID-teknologiaa sisältävän pesukoneen, ja joka on vaateostoksilla. Jos liike, josta vaatteet ostetaan, suorittaa niihin sammutuskäskyn ostohetkellä, ei asiakkaan kotona oleva pesukone voi lukea tunnisteita ja siten asettaa oikeaa pesuohjelmaa vaatteille. Silloin on suuri vaara, että juuri ostetut vaatteet menevätkin pi-

loille. Vaikka tämä ei varmastikaan ole aivan kriittisin esimerkki, antaa se hyvän käsityksen sammutuskäskyyn sisältyvistä ongelmista.

Sammutuskäskyä monesti parempi vaihtoehto on kuitenkin nukutuskäsky (*Sleep Command*). Se on huomattavasti kuluttajaystävällisempi, koska siinä ostopaikalla tunniste asetetaan vain väliaikaisesti pois käytöstä. Tässä tapauksessa asiakkaan on ostoksen jälkeen aktivoitava tunniste fyysisesti vaikkapa painamalla tiettyä nappia. Se, että tunnistetta ei voi aktivoida radioaalloilla, tuo mukanaan huomattavan määrän tietoturvaa. Kuitenkin tässäkin oletetaan, että vain asianomaiset henkilöt (asiakkaat) pääsevät käsiksi tunnisteeseen ja siten aktivoimaan sen. Haittapuolina voitaneen mainita ylimääräisen haitan, joka koituu asiakkaalle kun hänen täytyy aktivoida tunniste uudelleen, jotta hän voi käyttää tunnistetta edelleen hyödyksi. Toinen ehkäpä suurin haitta on tunnisteen hinta, joka todennäköisesti olisi korkeampi, koska tunnisteeseen täytyisi asentaa jonkinlainen kytkin aktivoimisen mahdollistamiseksi.

Loogisesti voitaisiin ajatella, että yksinkertaisesti kryptataan kaikki tieto, mitä tunniste lähettää. Siten voitaisiin ratkaista suuri osa koko tietoturvaongelmaa. Valitettavasti ratkaisu ei tässäkään tapauksessa ole näin yksioikoinen. Vahva kryptaus vaatii kohtuullisen paljon prosessointitehoa. Tämä nostaa taas tunnisteiden hintaa. Maailmassa, jossa melkein kaikissa kulutustuotteissa olisi RFID-tunniste, pitää niiden hintojenkin olla halpoja. 25 sentin tunnistetta ei vain voida laittaa 5 sentin voittomarginaalin tuotteeseen. On kuitenkin olemassa tuotteita, johon hieman kalliimpikin tunniste sopii. Esimerkiksi kannettavat sairaalalaitteet voivat maksaa kymmeniä tai jopa satojatuhansia dollareita. Näistä laitteista puhuttaessa hieman kalliimpikin tunniste on varmasti hyväksyttävissä. Tässä yhteydessä voitaisiin ajatella prosessointitehon kalleutta ja Mooren lakia. Jos kerran komponentteja saadaan piirilevylle kaksinkertainen määrä noin joka 18 kuukausi, niin silloin pitäisi myös teoriassa hyvällä prosessointiteholla varustettujen tunnisteiden hintojen alentua. Tämä voi pitää paikkansa pitemmän päälle mutta ei ole todennäköistä seuraavan kahden vuoden kuluessa.

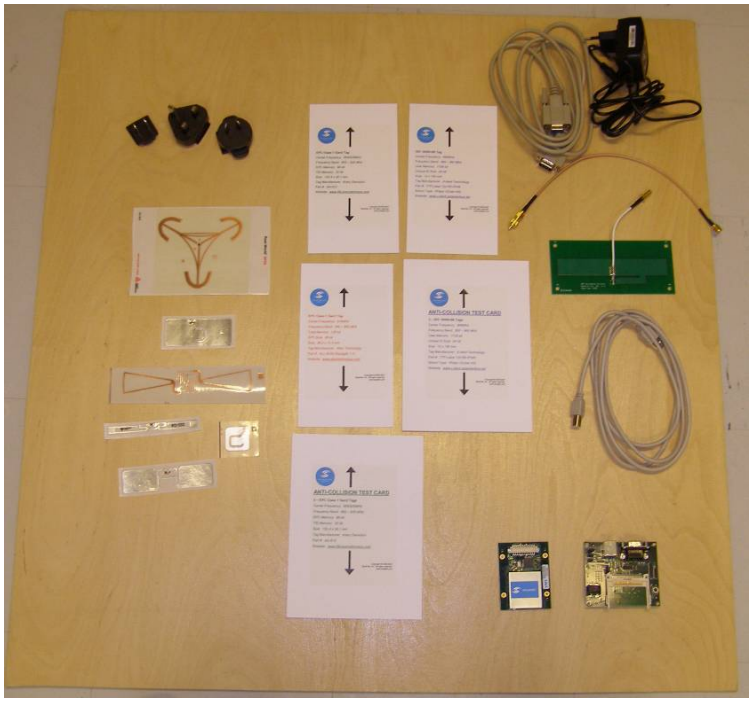
Yhteenvetona voitaisiin sanoa, että mikään näistä keinoista ei ratkaise kaikkia ongelmia. Erilaiset yhdistelmät tarjoavat eritasoisia ratkaisuja uhkia vastaan. Kuitenkin kaikkein tärkeintä on turvata yrityksen sisäinen tietojärjestelmä, käsittäen esimerkiksi tietokannat ja muut kriittiset osa-alueet. Tämä pätee tietysti, ei vain RFID-sovelluksiin, vaan myös kaikkiin IT-sovelluksiin, jotka käsittelevät tärkeää informaatiota.

6 Lukijan suunnittelu ja toteutus

Tämän tutkintotyön tavoitteisiin kuuluvan uuden RFID-lukijan suunnitteluun käytettiin SkyeTekin M9 Developer Kit RFID-kehityspakettia, jonka sisältö on nähtävissä kuvassa 14.

Vasemmalla kuvassa on nähtävissä verkkovirta-adapterit eri maihin sekä 6 erilaista EPC Class 1 Generation 1-, EPC Class 1 Generation 2- ja ISO 18000 - 6B -tunnistetta. Keskellä kuvassa ovat *Anti-Collision test Card* -lajitelma, jolla voidaan helposti testata usean eri tunnisteen lukeminen ja niistä syntyvät häiriöt. Ylhäällä oikealla on verkkovirtamuuntaja ja RS-232 kaapeli. Seuraavaksi niiden alla on antennin ja moduulin välinen kaapeli, UHF-antenni ja USB-kaapeli. Alhaalla oikealla on SkyeTek M9 -moduuli ja *Host Interface Board (*HIB*)*.

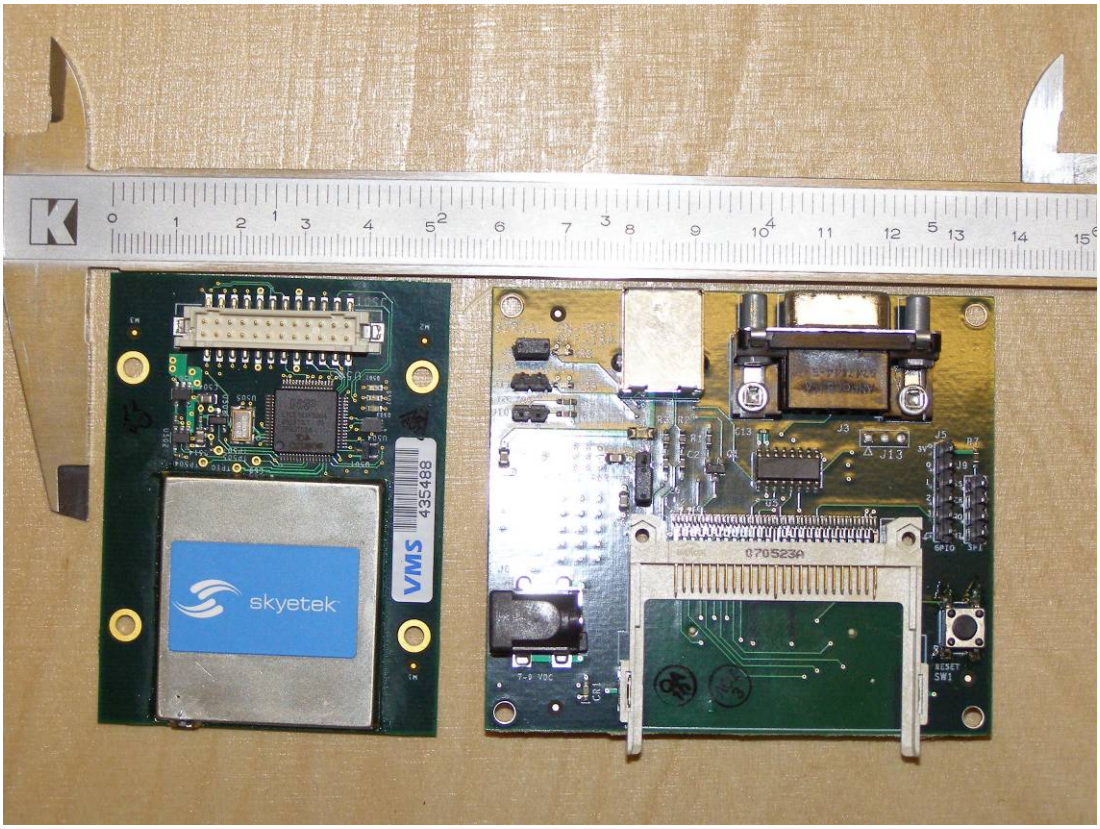
Kuvassa oleva antenni toimitetaan kohtuullisen suuressa (15x25x10 cm) muovikotelossa. Tämä kotelo purettiin pois jo heti ennen testausta, koska antennia oli huomattavasti parempi käsitellä siten kun se on esitetty kuvassa 14.



Kuva 14. Developer Kitin sisältö. /19/

Kuvassa 15 on esitettynä moduuli ja SkyeTekin tekemä HIB. Valmistaja on asettanut HIB:iin valmiiksi sekä RS-232 että USB 2.0 liitännät. Kortissa on myös ylimääräinen 7,0 V:n jännitteensyöttö, jolla mahdollistetaan moduulin käyttö maksimitehotasolla 27,0 dBm. USB 2.0 -liitännästä saatava 5,0 V:n jännite mahdollistaa moduulin käytön vain 20 dBm tehotasoilla ilman mahdollisia häiriöitä isäntäkoneen USB-portissa.

Moduulipiiri on erittäin pieni, joten se sopii erinomaisesti kannettaviin sovelluksiin. Pituutta piirillä on 69,6 mm ja leveyttä 53,1 mm. Tämä oli yksi syy siihen miksi juuri tämä moduuli valittiin projektiin mukaan. Toinen syy oli moduulin tarjoamien liitäntöjen monimuotoisuus. USB 2.0- ja RS-232 -liitäntämahdollisuudet antavat tulevaisuudessa mahdollisuuden kehitellä toisenlaisia tuotteita markkinoille. Ohjattavat I/O-liitännät, joita moduuli tarjoaa 4 kappaletta, antaa mahdollisuuden kehitellä tuotteelle lisäominaisuuksia, joita käsitellään tarkemmin tulevissa kappaleissa.



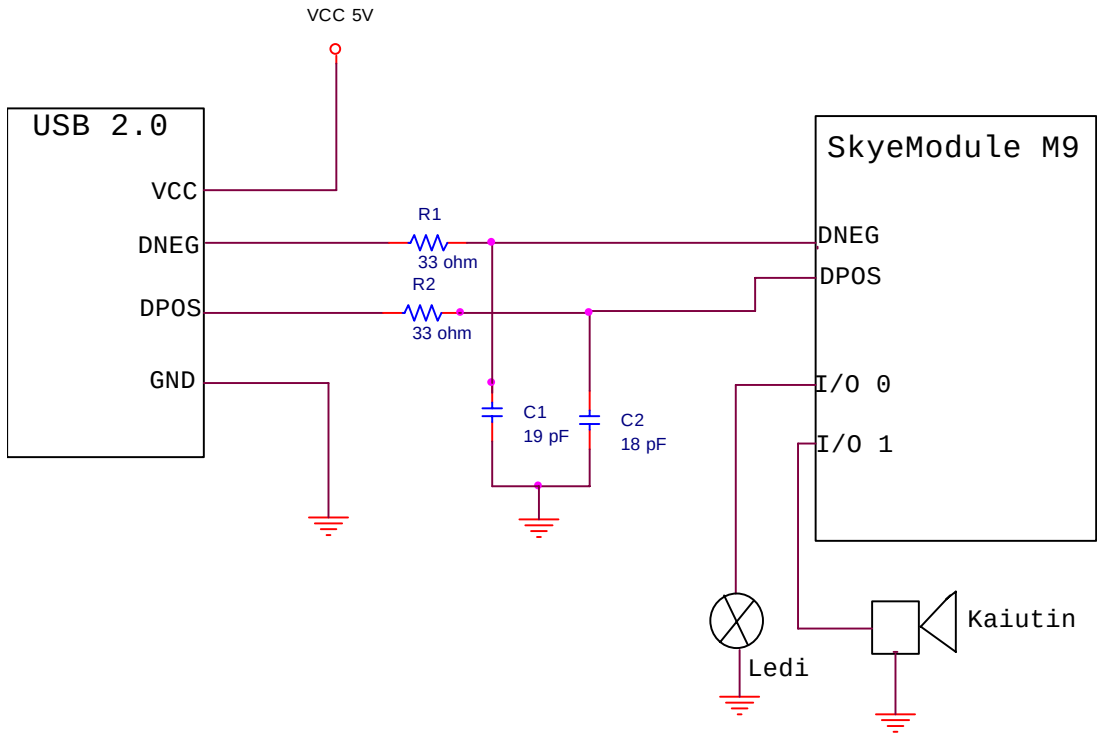
Kuva 15. Lukijamoduuli ja Host Interface Board. /19/

6.1 Moduulin kytkeminen USB 2.0 -liitäntään

Laitteen valmistuskustannuksien minimoimiseksi on USB 2.0 -liitäntä tehtävä ilman SkyeTekin HIB-piiriä. Isäntäkonetta ei voi kuitenkaan kytkeä suoraan USB-kaapelilla moduuliin, koska se voisi vahingoittaa porttia ja tehdä sen käyttökelvottomaksi. Tästä syystä täytyy isäntäkoneen ja lukijan välille rakentaa suodatinkytkentä, jonka tarkoitus on suojata isäntäkoneen USB-porttia.

DNEG-signaali ajetaan RC-suodattimen läpi, joka koostuu 33 Ω:n vastuksesta ja 19 pF:n kondensaattorista. DPOS-signaali ajetaan RC-suodattimen läpi, joka koostuu 33 Ω:n vastuksesta ja 18 pF:n kondensaattorista. Näin voidaan varmistaa, että laitetta on turvallista käyttää eikä siitä koidu haittaa isäntäkoneen porttiin.

RFID-lukija, joka ei ilmoita lukemastaan tunnisteesta mitenkään, ei olisi kovinkaan mielekäs käyttäjän näkökulmasta. Tästä syystä otetaan kaksi moduulin neljästä tarjoamasta I/O-liitännästä käyttöön ja asetetaan niihin ledi ja kaiutin. Näin välittyy myös käyttäjälle tieto heti kun yksi tunniste on saatu luettua. Kuva 16 esittää piirikaavion, joka mahdollistaa moduulin kytkemisen USB 2.0 -liitäntään ilman HIB-piiriä.



Kuva 16. Moduulin USB 2.0 suodinkytkentä ja I/O-liitännät. /20/

6.2 Ohjelma moduulille I/O-ohjaukseen

Moduulin I/O-liitäntöjen testaukseen tarvitsee moduulille tehdä oma ohjelmansa, jolla testauksen voi suorittaa. Ohjelmakoodi on esitettynä liitteessä 1. Ohjelmalla on tarkoitus ohjata I/O-liitäntöjä 1 ja 2 siten, että ne asetetaan output-tilaan. Ohjelmalla myös kytketään liitäntöihin jännite kun tunniste on luettu. Näin käyttäjä saa sekä ledillä että kaiuttimella tiedon siitä, että tunniste on luettu.

SkyeTekin tarjoamat valmiit kirjastot ja kooditiedostot saa käyttöön kun lisää SkyeTekApi.h:n, SkyeTekProtocol.h:n ja stapi.lib:n projektiin. Nämä tiedostot toimitetaan Developer Kitin mukana CD-levyllä.

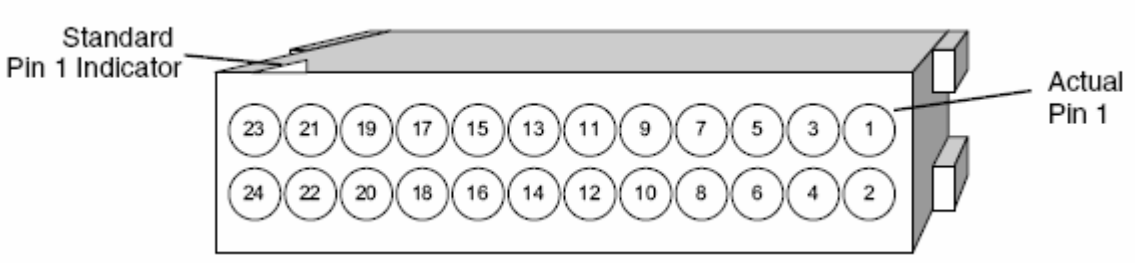
Ohjelman käynnistyttyä kaikki sekä sarja- että USB-porteissa olevat laitteet käydään läpi SkyeTek_DiscoverDevice:lla. Kaikki laitteet, jotka ovat kiinni isäntäkoneessa, toimitetaan SkyeTek_DiscoverReaders:lle. Tämä käy laitteet läpi ja tarkistaa oliko mikään laitteista lukija.

Lukijalaiteen löydyttyä voidaan asettaa I/O-liitäntöjen suunnat ja arvot. Suunta voidaan määrittää siten, että arvolla 00 voidaan määrittää liitäntä ulostuloksi. Liitäntöjen arvot voidaan määrittää siten, että binääriluvulla 10000011 saadaan aktivoitua I/O-liitännät sekä kytkettyä liitännät 1 ja 2 ”High”-tilaan. Ohjelmalle tämä luku täytyy kertoa heksadesimaalilukuna, joten vastaava arvo on 83.

Tunnisteiden käsittely voidaan suorittaa SkyeTek_SelectTag:lla. Tämä palauttaa ensimmäisen lukijan kuulustelualueella olevan tunnisteen. Jos halutaan käsitellä useampia tunnisteista, tarvitsee käyttää SkyeTek_SelectTags-funktiota. Tässä työssä esitetty testiohjelma ei hae kentästä kuin yhden tunnisteen ja kytkee ulostulot 1 ja 2 ”High”-tilaan.

6.3 Prototyypin testaus

Ensiksi prototyyppi UHF-lukijasta koottiin protolaudalle ja testattiin vain HIB-piirin ohittava kytkentä, eli kuvan 16 piiri mutta ilman I/O-kytkentöjä. Moduulipiirin 24-pinnisen liittimen jalkoihin juotettiin johtimet pinneihin 9 (VCC), 10 (GND), 11 (DNEG) ja 13 (DPOS). Kuva 17 esittää moduulipiirin liittimen pinnijärjestyksen.



Kuva 17. Moduulipiirin liittimen pinnijärjestys. /18/

SkyeWare 4.0 -ohjelmistoa käytettiin hyväksi kytkennän toimivuuden toteamiseksi. Lukija toimi aivan samalla tavoin kuin sitä oli käytetty HIB:n kanssa, joten kytkennän oikeellisuus ja toimivuus saatiin tarkistettua.

Seuraavaksi piiriä testattiin GPIOtest-ohjelmalla. SkyeTek on ilmoittanut, että I/O:n ollessa ”High”-tilassa, on siinä vähintään 2,9 V:n jännite. Yleismittarilla voitiin mitata pinneistä 21 (GPIO 0) ja 23 (GPIO 1) 3,24 V:n jännite, joten tältä osin voitiin myös ohjelman sekä moduulin toimivuus todeta. /18/

7 Yhteenveto

Tässä kappaleessa esitetään yhteenveto tehdystä työstä, arvioidaan saavutettuja tavoitteita, pohditaan työssä opittuja asioita ja esitetään työlle kehitys- ja jatkoideoita.

7.1 Tavoitteiden saavuttamisen arviointi

Ensiksikin työssä oli tavoitteena tutustua RFID-teknologiaan. Tämä onnistui hyvin ja kattavan lähdevalikoiman ansiosta työn tekijä sai hyvin yleiskuvan RFID:stä. Tästä on varmasti hyötyä työn tekijälle tulevaisuudessa.

UHF-lukijan osalta päästiin myös tavoitteisiin. Lukijan liittäminen USB 2.0 -liitäntään onnistui ilman HIB-piiriä ja moduulin I/O-liitäntöjä onnistuttiin käyttämään työssä omiin tarkoituksiin.

7.2 Työssä opittuja asioita

Työ oli monella tapaa opettavainen. Ensinnäkin jo edellä mainittu tutustuminen RFID-teknologiaan oli tietenkin välttämätöntä, jotta työ oli mahdollista suorittaa. Teknologiaan tutustuminen oli haastavaa mutta erittäin mielenkiintoista. RFID on esillä nykypäivänä ja juuri siksi sen tutkiminen on mielekästä. Työ opetti tekijälleen paljon uusia asioita RFID:stä ja herätti kasvavan mielenkiinnon aihepiiriä kohtaan.

Lukijan suunnittelu antoi uuden näkökulman RFID-teknologiaan. Se, että pääsi käytännössä työskentelemään ja rakentamaan uutta laitetta, auttoi ymmärtämään RFID:tä huomattavasti paremmin kuin se olisi ollut mahdollista pelkästään vain teoriapohjalta. Lukijalle tehty ohjelma, jolla ohjattiin I/O-liitäntöjä (liite 1), opetti myös lukijan eri mahdollisuuksista.

7.3 Kehitys ja jatko

Lukijan suunnittelun jälkeen luonnollinen jatko projektille olisi tietenkin tehdä siitä myytävä versio. Tätä varten lukijamoduuli olisi koteloitava sekä USB 2.0 -kytkentä olisi tehtävä piirille. Kytkentä olisi mahdollista sijoittaa vaikkapa liittimen sisään, joten se olisi mahdollista koota nopeasti kasaan. Lediä varten voitaisiin koteloon porata reikä, joka voisi näin ilmaista käyttäjälle, että tunniste on luettu kaiuttimen äänimerkin lisäksi.

Tuotetta kaupallistettaessa pitäisi tietysti lukijaa varten suunnitella graafinen käyttöliittymä, johon tieto tunnisteista tulisi. Koska lukijaa ohjataan nykyisessä muodossaan isäntäkoneen välityksellä, pitäisi käyttöliittymästä myös luonnollisesti ohjata lukijan toimintaa.

Lukijasta voisi tehdä myös kokonaan toisen tuotteen, joka toimisi RS-232 -liitännän kautta. Toinen uusi tuote voisi olla mikrokontrollerikytkennällä varustettu lukija, joka mahdollistaisi applikaatioiden tekemisen suoraan lukijalaitteeseen. Näin lukijaa ei tarvitsisi ohjata isäntäkoneella, vaan toiminnallisuus voitaisiin siirtää lukijalaitteeseen.

Lähteet

Painetut lähteet:

1. Finkenzeller, Klaus: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition. John Wiley & Sons, Ltd. 2003. 446 s.
2. Jones, Chung: RFID in Logistics. CRC Press. 2008. 489 s.
3. Bhatt, Glover: RFID Essentials. O'Reilly. 2006. 279 s.
4. Shepard, Steven: RFID Radio Frequency Identification. McGraw-Hill. 2005. 256 s.
5. Banks, Hanny, Pachano, Thompson: RFID Applied. John Wiley & Sons, Ltd. 2007. 509 s.

Sähköiset lähteet:

6. IT-World. [www-sivu]. [viitattu 4.3.2008] Saatavissa: http://mithras.itworld.com/download/book_chapters_and_wps/ibm_press/rfid_01fig25.gif
7. Interraction design. [www-sivu]. [viitattu 5.3.2008] Saatavissa: http://interactiondesign.files.wordpress.com/2006/03/ad%20rfid.jpg
8. Defence Logistics Agency. [www-sivu]. [viitattu 7.3.2008] Saatavissa: http://warfighter.dla.mil/contracting/rfid/rfidchip.jpg
9. Expoplanner. [www-sivu]. [viitattu 7.3.2008] Saatavissa: http://asis2007.expoplanner.com/featurepics/000689_AA-T200_Personnel_Badge_Tag.jpg
10. Wikipedia. [www-sivu]. [viitattu 14.3.2008] Saatavissa: http://en.wikipedia.org/wiki/ISO_11784_&_11785
11. RFID -news. [www-sivu]. [viitattu 15.3.2008] Saatavissa: http://www.rfidnews.com/iso_11784short.html
12. Wikipedia. [www-sivu]. [viitattu 15.3.2008] Saatavissa: http://en.wikipedia.org/wiki/Biometric_passport

13. Epc Finland. [www-sivu]. [viitattu 18.3.2008] Saatavissa: http://www.epcfinland.fi/ajankohtaista.html
14. RFID USA. [www-sivu]. [viitattu 19.3.2008] Saatavissa: http://rfidusa.com/superstore/pdf/Understanding_RFID_Frequencies.pdf
15. Scansource. [www-sivu]. [viitattu 19.3.2008] Saatavissa: http://www.scansource.com/europe/upload/RFID_Frequencies.pdf
16. Industrial News Room. [www-sivu]. [viitattu 30.3.2008] Saatavissa: http://news.thomasnet.com/IMT/archives/2006/04/rfid_tags_to_track_airborne_bags.html?t=archive
17. Texas Instruments. [www-sivu]. [viitattu 30.3.2008] Saatavissa: http://www.ti.com/rfid/shtml/prod-trans-RI-TRP-RR2B.shtml
18. SkyeTek, INC. SkyeTek M9 UHF-module dokumentaatio [sähköinen dokumentti]. [viitattu 13.5.2008]

Muu materiaali:

19. Ville Hirvimies. Kuva otettu 30.3.2008.
20. Ville Hirvimies. Piirikaaviosuunnittelu 20.4.2008.

Liitteet:

1. Testiohjelma GPIOtest.cpp:n ohjelmakoodi

```
#include "stdafx.h"
#include "SkyeTekAPI.h"
#include "SkyeTekProtocol.h"

// stop flag
bool isStop = false;
LPSKYETEK_READER lukijat[10];     //globaali muuttuja lukijoille, jota käytetään
                                  //SelectLoopCallback loopissa


unsigned char SelectLoopCallback(LPSKYETEK_TAG lpTag, void *user)
{
   if( !isStop )
  {
     if( lpTag != NULL )
       {
          printf("Tunniste: %s; Tyyppi: %s\n", lpTag->friendly,
          SkyeTek_GetTagTypeNameFromType(lpTag->type));
          SkyeTek_FreeTag(lpTag);

         //Merkataan lukijan GPIO-liitännät output-tilaan, allokoidaan muisti "dataOutPut"
         //muuttujalle sekä "dataOutPutHigh" muuttujalle. Merkataan I/O-liitännät 0 ja 1
         //high-tilaan (0x83)

          LPSKYETEK_DATA dataOutPut = NULL;
          dataOutPut = SkyeTek_AllocateData(1);
          dataOutPut->data[0] = 0x00;
          LPSKYETEK_DATA dataOutPutHigh = NULL;
          dataOutPutHigh = SkyeTek_AllocateData(1);
          dataOutPutHigh->data[0] = 0x83;

          SkyeTek_SetSystemParameter(lukijat[0], SYS_PORT_DIRECTION, dataOutPut);
          SkyeTek_SetSystemParameter(lukijat[0], SYS_PORT_VALUE, dataOutPutHigh);

           //Vapautetaan allokoitu muisti
           SkyeTek_FreeData(dataOutPut);
           SkyeTek_FreeData(dataOutPutHigh);

       }
   }
          return( !isStop );
}
```

```
DWORD WINAPI ThreadProc(LPVOID lpParameter)
{
   LPSKYETEK_DEVICE *devices = NULL;
   LPSKYETEK_READER *readers = NULL;
   SKYETEK_STATUS st;

    unsigned int numDevices;
    unsigned int numReaders;

    printf("Etsit\x84\x84n lukijoita...\n");

    while( !isStop )
    {
       numDevices = SkyeTek_DiscoverDevices(&devices)

       if( numDevices == 0 )
         {
            Sleep(100);
            continue;
         }

        if( isStop )
        return 1;

        numReaders = SkyeTek_DiscoverReaders(devices, numDevices, &readers);

        if( numReaders == 0 )
        {
          SkyeTek_FreeDevices(devices,numDevices);
          Sleep(100);
          continue;
        }
        break;
    }

   // Asetetaan lukijan tiedot
   printf("Lukija l\x94ytyi: %s\n\n", readers[0]->friendly);
   lukijat[0] = readers[0];                    //kopioidaan lukijan tiedot "lukija-muuttujaan"

   //Lukijan tunnistuessa outputit ”Low” tilaan

   LPSKYETEK_DATA dataOutPut = NULL;
   dataOutPut = SkyeTek_AllocateData(1);
   dataOutPut->data[0] = 0x00;

   LPSKYETEK_DATA dataOutPutHigh = NULL;
   dataOutPutHigh = SkyeTek_AllocateData(1);
   dataOutPutHigh->data[0] = 0x80;
```

```
    SkyeTek_SetSystemParameter(lukijat[0], SYS_PORT_DIRECTION, dataOutPut);
    SkyeTek_SetSystemParameter(lukijat[0], SYS_PORT_VALUE, dataOutPutHigh);

    SkyeTek_FreeData(dataOutPut);
    SkyeTek_FreeData(dataOutPutHigh);

    printf("Etsit\x84\x84n tunnisteita...\n\n");
    st = SkyeTek_SelectTags(readers[0],AUTO_DETECT,SelectLoopCallback,0,1,NULL);
    if( st != SKYETEK_SUCCESS )
    printf("Etsint\x84 ep\x84onnistui\n");
    printf("Etsint\x84 onnistui\n");

    // lukijoiden siivous
    SkyeTek_FreeReaders(readers, numReaders);
    SkyeTek_FreeDevices(devices, numDevices);
    return 1;
}

int main(int argc, char* argv[])
{
   DWORD id1;
   HANDLE h;
   char line[128];
   printf("SkyeTek M9 Module testiohjelma\n------------------------------\n\n");
   printf("Paina ENTER poistuaksesi\n\n");
   if( (h=CreateThread(NULL,0,ThreadProc,NULL,0,&id1)) == NULL )
   return FALSE;
   gets(line);
   CloseHandle(h);
   printf("Painoit ENTER, ohjelma on p\x84\x84ttynyt\n");
   isStop = true;
   return 0;
}
```